Jurnal Penelitian Nusantara
Volume 2 ; Nomor 4 ; April 2026 ; Page 295-307
Doi : https://doi.org/10.59435/menulis.v2i4.1104
Website : https://padangjurnal.web.id/index.php/menulis
E-ISSN : 3088-988X

Kekosongan Norma Hukum dalam Penanganan *Deepfake* sebagai Alat Kejahatan Siber: Studi Yuridis di Wilayah Polri Klungkung

I Putu Gede Aryawan

Mahasiswa Program Studi Ilmu Hukum, Fakultas Hukum, Ilmu Sosial, dan Ilmu Politik
Universitas Terbuka
Email: 048083075@ecampus.ut.ac.id

ABSTRAK

Perkembangan teknologi digital berbasis *artificial intelligence* telah melahirkan fenomena *deepfake* yang berpotensi disalahgunakan sebagai alat kejahatan siber, sementara hukum positif di Indonesia belum mengaturnya secara spesifik sehingga menimbulkan kekosongan norma hukum. Penelitian ini bertujuan untuk menganalisis pengaturan hukum positif terhadap penggunaan *deepfake* serta mengkaji konstruksi kekosongan norma hukum dalam praktik penegakan hukum oleh Polri di wilayah Klungkung. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, melalui studi kepustakaan terhadap bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa pengaturan hukum terhadap *deepfake* masih bersifat parsial dan hanya menjangkau akibat dari penyalahgunaannya melalui pasal-pasal umum dalam Undang-Undang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana. Selain itu, kekosongan norma hukum berdampak pada kesulitan pembuktian, ketidakpastian hukum, dan ketergantungan pada diskresi dalam praktik penegakan hukum. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif melalui perumusan regulasi yang secara eksplisit mengatur *deepfake* serta penguatan kapasitas aparat penegak hukum agar penanganan kejahatan siber dapat berjalan lebih efektif.

Kata kunci: *deepfake*, hukum pidana, kejahatan siber, kekosongan norma, penegakan hukum

PENDAHULUAN

Perkembangan teknologi digital dalam beberapa tahun terakhir menunjukkan dinamika yang sangat cepat dan cenderung sulit dikendalikan oleh sistem regulasi yang ada. Kusnadi dan Putri (2025) menjelaskan bahwa transformasi digital telah mengubah hampir seluruh aspek kehidupan manusia, termasuk dalam cara berkomunikasi dan mengakses informasi. Dalam konteks tersebut, kehadiran teknologi *Artificial Intelligence* menjadi salah satu pendorong utama percepatan inovasi digital yang semakin kompleks. Menurut Darmawan et al. (2025), teknologi berbasis *Artificial Intelligence* tidak hanya berfungsi sebagai alat bantu, tetapi telah berkembang menjadi sistem yang mampu mereplikasi pola pikir dan perilaku manusia dalam bentuk digital. Kondisi ini kemudian melahirkan berbagai inovasi baru, salah satunya adalah teknologi *deepfake* yang saat ini menjadi perhatian serius dalam kajian hukum modern. Arvitto (2025) menyebutkan bahwa *deepfake* merupakan bentuk manipulasi digital yang mampu menciptakan representasi visual dan audio seseorang secara realistis sehingga sulit dibedakan dari kenyataan.

Fenomena *deepfake* tidak lagi sekadar menjadi isu teknologi, melainkan telah berkembang menjadi persoalan hukum yang memiliki implikasi luas terhadap keamanan dan ketertiban masyarakat. Wanggai et al. (2026) mengemukakan bahwa penyalahgunaan teknologi *deepfake* telah meningkat secara signifikan dalam berbagai bentuk kejahatan digital. Dalam praktiknya, teknologi ini sering digunakan untuk melakukan penipuan, pencemaran nama baik, hingga penyebaran konten pornografi yang melibatkan identitas seseorang tanpa persetujuan. Hiariej, E. O. S. (2022), menegaskan bahwa dampak dari penyalahgunaan *deepfake* tidak hanya merugikan korban secara individu, tetapi juga dapat mengganggu stabilitas sosial akibat penyebaran informasi yang menyesatkan. Bahkan, Noerman & Ibrahim (2024) menambahkan bahwa keberadaan *deepfake* berpotensi merusak kepercayaan publik terhadap informasi digital yang beredar di masyarakat.

Dalam perspektif hukum pidana, perkembangan teknologi *deepfake* menghadirkan tantangan baru yang tidak dapat diabaikan. Prayoga (2025) menjelaskan bahwa hukum pidana pada dasarnya dibangun atas asas legalitas yang mengharuskan setiap perbuatan pidana diatur secara jelas dalam peraturan perundang-undangan. Namun demikian, perkembangan teknologi yang sangat cepat sering kali tidak diikuti oleh pembaruan hukum yang memadai. Prasetyo, T. (2023)., menyatakan bahwa regulasi yang ada saat ini, seperti Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik, belum secara spesifik mengatur mengenai *deepfake* sebagai bentuk kejahatan siber. Kondisi ini menyebabkan adanya kesenjangan antara perkembangan teknologi dengan kemampuan hukum dalam mengaturnya.

Ketiadaan pengaturan yang spesifik mengenai *deepfake* dalam hukum positif Indonesia menunjukkan adanya kekosongan norma hukum atau *legal vacuum*. Kusnadi dan Putri (2025) menjelaskan bahwa kekosongan norma terjadi כאשר hukum tidak mampu menjangkau fenomena baru yang berkembang di masyarakat. Dalam konteks *deepfake*, kekosongan norma ini berdampak pada kesulitan dalam menentukan dasar hukum yang tepat untuk menjerat pelaku. Sihotang, H. (2024), menegaskan bahwa aparat penegak hukum sering kali harus menggunakan pasal-pasal yang bersifat umum untuk menangani kasus *deepfake*, meskipun pasal tersebut tidak secara langsung relevan dengan karakteristik kejahatan yang terjadi. Hal ini menunjukkan bahwa sistem hukum belum sepenuhnya adaptif terhadap perkembangan teknologi digital.

Selain permasalahan norma hukum, aspek pembuktian dalam kasus *deepfake* juga menjadi tantangan tersendiri dalam praktik penegakan hukum. Darmawan et al. ((2025) menyatakan bahwa bukti digital yang dihasilkan melalui teknologi *deepfake* memiliki tingkat kompleksitas yang tinggi sehingga sulit diverifikasi keasliannya. Devi (2026) menjelaskan bahwa dalam sistem hukum pidana, pembuktian merupakan elemen penting yang menentukan dapat tidaknya seseorang dipidana. Namun, dalam kasus *deepfake*, pembuktian menjadi semakin sulit karena teknologi tersebut mampu memanipulasi identitas secara sangat realistis.

Kondisi ini menimbulkan potensi kesalahan dalam penegakan hukum apabila tidak didukung oleh kemampuan forensik digital yang memadai.

Peningkatan jumlah kasus kejahatan berbasis teknologi digital menunjukkan bahwa fenomena *deepfake* telah menjadi ancaman nyata dalam kehidupan masyarakat modern. Wanggai et al. (2026) mengungkapkan bahwa tren kejahatan siber terus mengalami peningkatan seiring dengan berkembangnya teknologi digital. Hukmana (2025) menambahkan bahwa kejahatan berbasis *deepfake* memiliki karakteristik yang berbeda dibandingkan dengan kejahatan konvensional karena melibatkan teknologi yang canggih dan sulit dilacak. Kondisi ini menuntut adanya respon hukum yang lebih progresif dan adaptif agar mampu mengimbangi perkembangan teknologi yang ada.

Dalam praktik penegakan hukum di tingkat kepolisian, khususnya di wilayah Klungkung, fenomena kejahatan siber mulai menunjukkan tren yang perlu mendapatkan perhatian serius (Flora, H. S. 2024). Aparat kepolisian dituntut untuk mampu memahami tidak hanya aspek hukum, tetapi juga aspek teknis dari kejahatan yang terjadi. Fauzi (2025) menjelaskan bahwa penegakan hukum terhadap kejahatan siber memerlukan pendekatan yang berbeda dibandingkan dengan kejahatan konvensional. Selain itu, (Kusnadi, S. A. Et al, 2025) menekankan bahwa aparat penegak hukum harus memiliki kemampuan adaptasi yang tinggi dalam menghadapi perkembangan teknologi yang semakin kompleks. Hal ini menunjukkan bahwa peran kepolisian menjadi sangat strategis dalam menangani kejahatan berbasis *deepfake*.

Kekosongan norma hukum dalam penanganan *deepfake* berpotensi menimbulkan ketidakpastian hukum atau *legal uncertainty*. Arvitto (2025) menyatakan bahwa ketidakpastian hukum dapat mengakibatkan lemahnya perlindungan terhadap korban serta tidak optimalnya penegakan hukum terhadap pelaku. Noerman & Ibrahim (2024) menambahkan bahwa dalam sistem hukum yang ideal, setiap perbuatan yang merugikan harus memiliki dasar hukum yang jelas agar dapat diproses secara adil. Namun, dalam kasus *deepfake*, ketiadaan norma yang spesifik menyebabkan adanya ruang interpretasi yang luas bagi aparat penegak hukum. Kondisi ini berpotensi menimbulkan perbedaan dalam penerapan hukum di lapangan.

Dengan demikian, dapat dipahami bahwa permasalahan *deepfake* tidak hanya berkaitan dengan aspek teknologi, tetapi juga menyentuh aspek fundamental dalam sistem hukum, yaitu kepastian, keadilan, dan kemanfaatan hukum. Rahman, A. (2025), menegaskan bahwa hukum harus mampu beradaptasi dengan perkembangan teknologi agar tetap relevan dalam mengatur kehidupan masyarakat. Kusnadi dan Putri (2025) juga menyatakan bahwa pembentukan regulasi yang responsif terhadap perkembangan teknologi menjadi kebutuhan mendesak dalam era digital saat ini. Oleh karena itu, penelitian mengenai kekosongan norma hukum dalam penanganan *deepfake* menjadi penting untuk dilakukan, khususnya dalam konteks penegakan hukum oleh kepolisian di wilayah Klungkung, guna memberikan kontribusi dalam pengembangan hukum pidana siber yang lebih adaptif dan responsif terhadap tantangan zaman.

Berdasarkan uraian latar belakang yang telah menegaskan adanya persoalan *legal vacuum* dalam penanganan *deepfake*, penting untuk menelaah berbagai penelitian terdahulu guna melihat posisi dan kontribusi penelitian ini secara lebih jelas. Penelitian yang dilakukan oleh Arvitto (2025) mengkaji implikasi hukum penggunaan *deepfake* dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik, dengan menekankan bahwa regulasi yang ada masih bersifat umum dan belum mampu menjangkau kompleksitas kejahatan berbasis *Artificial Intelligence*. Hasil penelitian tersebut menunjukkan bahwa aparat penegak hukum cenderung menggunakan pendekatan interpretatif terhadap pasal-pasal yang tersedia, sehingga berpotensi menimbulkan ketidakpastian hukum dalam praktiknya.

Selanjutnya, penelitian oleh Kusnadi dan Putri (2025) berfokus pada analisis kekosongan norma hukum dalam kejahatan siber berbasis teknologi mutakhir. Dalam kajiannya, disebutkan bahwa perkembangan teknologi seperti *deepfake* tidak diikuti dengan pembaruan regulasi yang memadai, sehingga menimbulkan kesenjangan antara hukum dan realitas sosial. Penelitian ini juga menyoroti perlunya pembentukan norma hukum baru yang lebih adaptif terhadap perkembangan teknologi digital, terutama dalam rangka menjamin kepastian hukum dan perlindungan terhadap korban.

Penelitian lain yang relevan dilakukan oleh Darmawan et al. (2025) yang mengkaji aspek pembuktian dalam kejahatan siber berbasis *Artificial Intelligence*. Dalam penelitiannya, Darmawan et al. menekankan bahwa bukti digital yang dihasilkan melalui teknologi *deepfake* memiliki tingkat kompleksitas yang tinggi, sehingga memerlukan pendekatan forensik digital yang lebih canggih. Hasil penelitian ini menunjukkan bahwa sistem pembuktian hukum yang ada saat ini masih memiliki keterbatasan dalam mengakomodasi karakteristik bukti digital yang terus berkembang.

Sementara itu, Noerman & Ibrahim (2024)dalam penelitiannya menyoroti dampak sosial dari penyalahgunaan *deepfake*, khususnya dalam konteks penyebaran disinformasi dan pencemaran nama baik. Penelitian tersebut menemukan bahwa *deepfake* dapat merusak kepercayaan publik terhadap informasi digital dan berpotensi menciptakan instabilitas sosial. Selain itu, penelitian ini juga menekankan pentingnya peran negara dalam memberikan perlindungan hukum terhadap masyarakat dari ancaman kejahatan berbasis teknologi digital.

Penelitian oleh Wanggai et al. (2026) kemudian melengkapi perspektif sebelumnya dengan mengkaji tren peningkatan kejahatan siber berbasis teknologi digital, termasuk *deepfake*. Dalam penelitiannya, disebutkan bahwa kejahatan berbasis *deepfake* menunjukkan peningkatan signifikan dalam beberapa tahun terakhir dan memiliki karakteristik yang berbeda dari kejahatan konvensional. Penelitian ini menegaskan bahwa diperlukan pendekatan hukum yang lebih progresif dan responsif untuk menghadapi perkembangan kejahatan siber yang semakin kompleks.

Berdasarkan uraian penelitian terdahulu tersebut, dapat dilihat bahwa sebagian besar penelitian masih berfokus pada aspek umum, seperti analisis regulasi, pembuktian, dan dampak sosial dari *deepfake*. Namun, penelitian-penelitian tersebut belum secara spesifik mengkaji bagaimana kekosongan norma

hukum tersebut dihadapi dalam praktik penegakan hukum di tingkat kepolisian, khususnya pada konteks wilayah tertentu. Oleh karena itu, penelitian ini memiliki kebaruan (*novelty*) dengan menitikberatkan pada analisis kekosongan norma hukum dalam penanganan *deepfake* sebagai alat kejahatan siber dari perspektif praktik penegakan hukum oleh Polri di wilayah Klungkung. Dengan demikian, penelitian ini tidak hanya bersifat konseptual, tetapi juga berupaya memberikan gambaran yang lebih konkret dan kontekstual mengenai tantangan yang dihadapi aparat penegak hukum dalam menghadapi fenomena kejahatan berbasis teknologi digital.

Berdasarkan latar belakang yang telah diuraikan, Rumusan Masalah dalam penelitian ini ialah. **1).** Bagaimana pengaturan hukum positif di Indonesia dalam mengakomodasi penggunaan *deepfake* sebagai alat kejahatan siber, khususnya ditinjau dari ketentuan dalam KUHP dan Undang-Undang Informasi dan Transaksi Elektronik ? **2).** Bagaimana konstruksi kekosongan norma hukum (*legal vacuum*) dalam penanganan *deepfake* serta implikasinya terhadap praktik penegakan hukum oleh Polri di wilayah Klungkung ?

Sejalan dengan rumusan masalah tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam pengaturan hukum positif yang berlaku dalam menangani kejahatan berbasis *deepfake*, serta mengidentifikasi keterbatasan norma hukum yang ada. Selain itu, penelitian ini juga bertujuan untuk mengkaji konstruksi kekosongan norma hukum dalam praktik penegakan hukum oleh Polri di wilayah Klungkung, sekaligus merumuskan konsep pengaturan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi digital. Penelitian ini diharapkan memberikan manfaat secara teoritis dan praktis. Secara teoritis, penelitian ini berkontribusi dalam pengembangan kajian hukum pidana siber, khususnya terkait kekosongan norma hukum (*legal vacuum*) dalam penanganan *deepfake*. Secara praktis, penelitian ini dapat menjadi referensi bagi aparat penegak hukum, khususnya Polri di wilayah Klungkung, dalam memahami dan menangani kejahatan berbasis *deepfake*. Selain itu, penelitian ini juga diharapkan dapat menjadi bahan pertimbangan bagi pembentuk kebijakan dalam merumuskan regulasi yang lebih adaptif terhadap perkembangan teknologi digital.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis normatif yang berfokus pada kajian terhadap norma hukum yang berlaku, khususnya dalam menganalisis kekosongan norma (*legal vacuum*) terkait penanganan *deepfake* sebagai alat kejahatan siber. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*) guna memahami secara komprehensif permasalahan hukum yang diteliti. Sumber bahan hukum terdiri dari bahan hukum primer berupa Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik, bahan hukum sekunder berupa buku dan jurnal ilmiah yang

relevan, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan, sedangkan metode analisis yang digunakan adalah analisis kualitatif dengan menggunakan teknik penafsiran hukum, baik secara gramatikal maupun sistematis, untuk memperoleh kesimpulan yang logis dan sesuai dengan tujuan penelitian.

HASIL DAN PEMBAHASAN

1. Pengaturan Hukum terhadap *Deepfake* sebagai Alat Kejahatan Siber di Indonesia

Berdasarkan hasil penelitian, dapat ditemukan bahwa hukum positif di Indonesia hingga saat ini belum merumuskan *deepfake* sebagai tindak pidana yang berdiri sendiri. Baik dalam UU Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE maupun dalam UU Nomor 1 Tahun 2023 tentang KUHP, tidak ditemukan definisi normatif yang secara eksplisit menyebut *deepfake* sebagai objek pengaturan pidana. Kondisi ini menunjukkan bahwa perkembangan teknologi *artificial intelligence* telah bergerak lebih cepat dibandingkan kemampuan pembentuk undang-undang dalam merumuskan norma yang spesifik.

Dalam konteks hukum pidana, keadaan demikian menimbulkan persoalan serius karena kejahatan tidak lagi hanya dilakukan melalui cara-cara konvensional, melainkan juga melalui rekayasa visual, audio, dan identitas digital yang sangat meyakinkan. Di titik ini, *deepfake* tidak dapat dipandang hanya sebagai bentuk manipulasi teknologi biasa, melainkan telah berkembang menjadi instrumen kejahatan siber yang berpotensi merugikan kehormatan, privasi, keamanan, bahkan ketertiban umum. Temuan ini juga diperkuat oleh kajian yang menyebut bahwa Indonesia masih mengalami kekosongan hukum karena belum adanya regulasi spesifik mengenai manipulasi data visual berbasis *AI*, sehingga penegakan hukum masih bergantung pada pasal-pasal umum yang tidak sepenuhnya selaras dengan sifat manipulasi algoritmik itu sendiri.

Secara normatif, rezim hukum yang paling dekat untuk menjerat penyalahgunaan *deepfake* saat ini adalah UU ITE. Namun, dari hasil analisis, UU ITE sesungguhnya lebih banyak mengatur akibat hukum dari penyebaran konten elektronik, bukan secara khusus mengatur rekayasa identitas digital berbasis *AI*. Salah satu fondasi penting yang tersedia adalah Pasal 5 UU ITE yang menegaskan keberadaan Informasi Elektronik dan/atau Dokumen Elektronik diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum, terutama dalam pembuktian perbuatan hukum yang dilakukan melalui sistem elektronik. Ketentuan ini penting karena hampir seluruh perkara *deepfake* berpusat pada objek digital, seperti video, gambar, suara, atau kombinasi ketiganya. Akan tetapi, pengakuan terhadap alat bukti elektronik tidak otomatis berarti bahwa hukum telah selesai mengatur *deepfake*. Pengakuan pembuktian hanya menyelesaikan satu sisi persoalan, yaitu sisi *evidence*, sedangkan sisi perumusan delik sebagai bagian dari hukum pidana materiil masih tetap menyisakan celah. Dengan demikian, hasil penelitian ini menunjukkan bahwa hukum

acara elektronik di Indonesia relatif sudah memiliki pijakan, tetapi hukum pidana materiilnya belum benar-benar siap mengakomodasi *deepfake* sebagai modus kejahatan baru.

Apabila dikaitkan dengan Pasal 27 ayat (1) UU ITE, norma ini dapat digunakan ketika *deepfake* diproduksi dan disebarkan dalam bentuk yang melanggar kesusilaan. Penjelasan resmi UU ITE menyebut bahwa yang dimaksud dengan "melanggar kesusilaan" adalah perbuatan mempertunjukkan ketelanjangan, alat kelamin, dan aktivitas seksual yang bertentangan dengan nilai-nilai yang hidup dalam masyarakat. Dalam praktik, ketentuan ini memang paling dekat untuk menjerat *deepfake pornography*, yakni ketika wajah korban direkayasa dan ditempelkan ke dalam konten seksual.

Bahkan ketentuan pidananya juga cukup tegas, karena Pasal 45 ayat (1) mengatur ancaman pidana bagi pihak yang menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya muatan yang melanggar kesusilaan. Namun, dari sudut analisis hukum, jangkauan norma ini tetap terbatas. Pasal tersebut hanya efektif pada kasus *deepfake* yang berunsur seksual, sedangkan *deepfake* sendiri memiliki bentuk yang jauh lebih luas, misalnya untuk penipuan, fitnah, manipulasi politik, penyamaran identitas, atau penggiringan opini. Artinya, Pasal 27 ayat (1) UU ITE hanya menjangkau salah satu cabang dari penyalahgunaan *deepfake*, bukan keseluruhan fenomenanya. Di sinilah tampak bahwa hukum positif Indonesia masih bekerja secara parsial dan belum mengenali *deepfake* sebagai kategori bahaya tersendiri.

Pasal 27A UU ITE dapat diposisikan sebagai norma yang relevan ketika *deepfake* digunakan untuk menyerang kehormatan atau nama baik seseorang. Secara normatif, pasal ini mengatur perbuatan menyerang kehormatan dengan cara menuduhkan suatu hal agar diketahui umum melalui media elektronik. Dalam praktik, ketentuan ini memang tampak sesuai untuk kasus *deepfake* yang menampilkan korban seolah-olah melakukan tindakan tercela. Namun, unsur "menuduhkan suatu hal" dalam pasal tersebut masih berlandaskan pada konsep penghinaan konvensional, sementara *deepfake* tidak selalu berupa pernyataan langsung, melainkan manipulasi visual dan audio yang membentuk realitas semu. Dengan demikian, Pasal 27A dapat digunakan sebagai dasar alternatif, tetapi belum cukup memadai untuk menjangkau keseluruhan karakter kejahatan *deepfake*, sehingga penerapannya masih bersifat kasuistis dan bergantung pada interpretasi penegak hukum.

Pasal 27B UU ITE relevan dalam kasus *deepfake* yang berkembang menjadi ancaman, pemerasan, atau *sextortion*, karena konten manipulatif dapat digunakan untuk menekan korban. Namun, pasal ini hanya menjerat akibat lanjutan berupa ancaman atau pemaksaan, bukan mengatur *deepfake* sebagai alat kejahatan itu sendiri. Oleh karena itu, Pasal 27B lebih tepat dipahami sebagai norma turunan yang belum mampu menjangkau keseluruhan praktik *deepfake*, terutama karena pelaku pembuat dan penyebar konten bisa berbeda. Di luar itu, Pasal 28 ayat (1) dan Pasal 28 ayat (3) UU ITE juga dapat dipertimbangkan dalam perkara tertentu. Pasal 28 ayat (1) mengatur distribusi atau transmisi informasi bohong atau menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam transaksi elektronik, sedangkan Pasal 28 ayat

(3) mengatur penyebaran pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat. Kedua norma ini menunjukkan bahwa UU ITE sebenarnya sudah memiliki perhatian terhadap bahaya informasi palsu. Namun, dari hasil analisis, penerapannya pada *deepfake* tetap tidak sederhana.

Pasal 28 ayat (1) mensyaratkan adanya kerugian materiel bagi konsumen dalam transaksi elektronik, sehingga hanya relevan pada *deepfake* yang benar-benar dipakai dalam konteks penipuan transaksi. Sementara itu, Pasal 28 ayat (3) mensyaratkan adanya kerusuhan di masyarakat, dan penjelasan resmi UU ITE menegaskan bahwa "kerusuhan" yang dimaksud adalah kondisi yang mengganggu ketertiban umum di ruang fisik, bukan di ruang digital atau siber. Artinya, tidak semua *deepfake* dapat ditarik ke norma ini. Banyak *deepfake* justru merusak reputasi pribadi, menimbulkan rasa malu, merusak kepercayaan, atau menciptakan kerugian psikologis tanpa sampai menimbulkan kerusuhan fisik di masyarakat. Di titik ini terlihat jelas bahwa hukum positif Indonesia lebih siap mengatur akibat tertentu dari berita bohong, tetapi belum siap mengatur *deepfake* sebagai teknologi fabrikasi realitas yang dapat merugikan korban tanpa selalu memenuhi seluruh unsur delik yang ada.

Jika dianalisis dari perspektif KUHP nasional, persoalan *deepfake* pada dasarnya masih menghadapi kendala yang sama. Meskipun UU Nomor 1 Tahun 2023 tentang KUHP menjadi bagian penting dari pembaruan hukum pidana, rumusan deliknya tetap bersifat umum, seperti penghinaan, penipuan, pemalsuan, pengancaman, dan tindak pidana terhadap ketertiban umum. Padahal, *deepfake* dapat muncul dalam berbagai bentuk dan tidak selalu cocok dimasukkan ke satu jenis delik tertentu. Karena itu, penggunaan pasal-pasal umum dalam KUHP masih dimungkinkan, tetapi belum cukup spesifik untuk menjawab *deepfake* sebagai kejahatan digital tersendiri. Kondisi ini menunjukkan adanya *legal lag*, yaitu ketika perkembangan teknologi bergerak lebih cepat daripada kemampuan hukum untuk mengaturnya.

Dilihat dari asas legalitas, persoalan tersebut menjadi semakin penting. Asas legalitas menuntut agar perbuatan pidana dirumuskan secara jelas, tegas, dan tidak multitafsir. Menariknya, pembentuk undang-undang sendiri dalam konsideran dan penjelasan umum UU Nomor 1 Tahun 2024 mengakui bahwa penerapan UU ITE sebelumnya masih menimbulkan multitafsir, kontroversi, dan perbedaan pemahaman terhadap beberapa pasal. Pengakuan resmi ini justru menguatkan argumentasi penelitian bahwa jika pasal-pasal umum dalam UU ITE masih rentan menimbulkan banyak tafsir, maka penggunaannya untuk menjerat *deepfake* yang jauh lebih kompleks tentu berisiko menimbulkan ketidakpastian hukum yang lebih besar. Dari sini tampak bahwa persoalan *deepfake* bukan hanya soal kurangnya pasal, tetapi juga soal kecocokan struktur norma dengan sifat kejahatannya. Norma yang terlalu umum akan membuat batas antara konten satir, *editing* biasa, ekspresi kreatif, dan rekayasa berbahaya menjadi kabur. Akibatnya, penegakan hukum berpotensi tidak seragam dan bergantung terlalu jauh pada interpretasi subyektif aparat.

Dalam kaitannya dengan penelitian terdahulu, hasil penelitian ini memiliki titik temu sekaligus titik beda. Penelitian yang terbit pada 2026 mengenai kekosongan hukum penipuan *deepfake* terhadap pejabat publik menegaskan bahwa instrumen hukum positif Indonesia masih menunjukkan kesenjangan norma

yang signifikan, khususnya karena pasal yang ada masih mensyaratkan unsur-unsur yang tidak selalu cocok dengan modus *deepfake*. Temuan itu sejalan dengan penelitian ini yang juga melihat bahwa pasal-pasal yang tersedia lebih banyak mengatur akibat tertentu, bukan mengatur *deepfake* sebagai teknik kejahatan. Demikian pula kajian tentang pertanggungjawaban pidana *deepfake porn* berbasis *AI* menyimpulkan bahwa regulasi Indonesia masih berfokus pada pornografi umum, sehingga belum mampu menjawab secara tuntas kekhasan manipulasi seksual berbasis teknologi. Penelitian lain juga menyatakan bahwa Indonesia masih mengalami *legal vacuum* karena belum ada regulasi spesifik mengenai manipulasi visual berbasis *AI*. Bedanya, penelitian ini tidak berhenti pada penjelasan konseptual tentang kekosongan norma, tetapi secara lebih rinci membedah satu per satu norma yang saat ini paling mungkin dipakai, lalu menunjukkan batas jangkau masing-masing pasal secara sistematis. Dengan demikian, kebaruan penelitian ini terletak pada penegasan bahwa masalah utama bukan sekadar tidak adanya aturan, melainkan ketidakcocokan antara struktur norma yang tersedia dengan karakter *deepfake* sebagai fabrikasi realitas digital.

Berdasarkan seluruh uraian tersebut, hasil penelitian ini menegaskan bahwa pengaturan hukum terhadap *deepfake* sebagai alat kejahatan siber di Indonesia masih bersifat parsial, tidak langsung, dan belum memadai. UU ITE memang menyediakan beberapa pasal yang dapat digunakan secara alternatif, seperti Pasal 27 ayat (1), Pasal 27A, Pasal 27B, serta Pasal 28 ayat (1) dan ayat (3), sementara KUHP dapat dipakai melalui delik-delik umum yang bersesuaian. Akan tetapi, seluruh pendekatan itu pada dasarnya masih bekerja setelah *deepfake* menimbulkan akibat tertentu.

Hukum positif Indonesia belum merumuskan *deepfake* sebagai perbuatan yang sejak awal dipandang berbahaya karena kemampuannya memalsukan realitas, menyalahgunakan identitas, dan merusak kepastian pembuktian. Dalam keadaan seperti ini, aparat penegak hukum tetap dapat bertindak, tetapi dasar tindakannya sangat bergantung pada konstruksi pasal yang dipilih dan penafsiran yang digunakan. Dari sudut kepastian hukum, ini adalah kelemahan yang mendasar. Oleh karena itu, pembaruan hukum yang dibutuhkan ke depan bukan sekadar menambah ancaman pidana, melainkan merumuskan norma yang secara eksplisit mendefinisikan *deepfake*, membedakan jenis penyalahgunaannya, dan menyesuaikan unsur deliknya dengan karakter kejahatan digital berbasis *artificial intelligence*.

2. Konstruksi Kekosongan Norma Hukum dalam Penanganan *Deepfake* oleh Polri

Beranjak dari hasil pembahasan sebelumnya yang menunjukkan bahwa pengaturan hukum terhadap *deepfake* masih bersifat parsial, maka rumusan masalah kedua berfokus pada bagaimana konstruksi kekosongan norma hukum (*legal vacuum*) tersebut muncul dan berdampak dalam praktik penegakan hukum, khususnya oleh Polri di wilayah Klungkung. Berdasarkan hasil penelitian, kekosongan norma hukum dalam konteks *deepfake* tidak hanya disebabkan oleh ketiadaan regulasi yang eksplisit, tetapi juga oleh ketidaksesuaian struktur norma yang ada dengan karakteristik kejahatan berbasis *artificial*

intelligence. Dengan kata lain, masalahnya bukan sekadar "tidak ada aturan", melainkan "aturan yang ada tidak mampu menjangkau realitas yang berkembang".

Secara konseptual, kekosongan norma hukum (*legal vacuum*) terjadi כאשר hukum tidak mampu mengatur fenomena sosial baru secara efektif. Dalam konteks *deepfake*, kekosongan tersebut dapat diidentifikasi melalui tiga indikator utama. Pertama, tidak adanya definisi hukum yang jelas mengenai *deepfake*, sehingga batas antara manipulasi digital biasa dan rekayasa berbahaya menjadi kabur. Kedua, tidak adanya rumusan delik yang secara khusus mengatur perbuatan menciptakan, menyebarkan, atau menggunakan *deepfake* sebagai sarana kejahatan. Ketiga, belum adanya standar pembuktian yang secara spesifik dirancang untuk mengidentifikasi dan memverifikasi konten berbasis *artificial intelligence*. Ketiga indikator ini menunjukkan bahwa kekosongan norma dalam kasus *deepfake* bersifat struktural, bukan sekadar teknis.

Dalam praktik penegakan hukum, kondisi tersebut berdampak langsung terhadap kinerja aparat kepolisian. Berdasarkan analisis, Polri dalam menangani kasus yang mengandung unsur *deepfake* cenderung menggunakan pendekatan *case by case* dengan memanfaatkan pasal-pasal yang dianggap paling mendekati. Pendekatan ini memang memberikan fleksibilitas, namun di sisi lain juga menimbulkan ketidakpastian hukum karena tidak adanya standar yang baku dalam menentukan konstruksi pasal. Dalam beberapa situasi, suatu perbuatan dapat dikualifikasikan sebagai pencemaran nama baik, sementara dalam kasus lain dapat dikategorikan sebagai penipuan atau bahkan tidak dapat diproses sama sekali karena tidak memenuhi unsur delik yang ada. Hal ini menunjukkan bahwa penegakan hukum terhadap *deepfake* sangat bergantung pada interpretasi aparat, bukan pada kepastian norma.

Dari perspektif teori penegakan hukum, kondisi tersebut menunjukkan adanya ketidakseimbangan antara tiga unsur utama, yaitu substansi hukum, struktur hukum, dan budaya hukum. Substansi hukum dalam hal ini belum mampu memberikan landasan yang jelas, sementara struktur hukum (aparat penegak hukum) dituntut untuk tetap menjalankan fungsi penegakan hukum dalam kondisi norma yang tidak memadai. Akibatnya, aparat kepolisian sering berada dalam posisi dilematis antara menegakkan hukum secara progresif atau tetap berpegang pada prinsip legalitas yang ketat. Dalam konteks ini, diskresi kepolisian menjadi salah satu instrumen yang sering digunakan untuk menjembatani kekosongan norma tersebut.

Namun demikian, penggunaan diskresi dalam penegakan hukum tidak dapat dijadikan solusi jangka panjang. Hal ini karena diskresi pada dasarnya merupakan kewenangan terbatas yang harus tetap berada dalam koridor hukum yang berlaku. Apabila diskresi digunakan secara berlebihan tanpa didukung oleh norma yang jelas, maka berpotensi menimbulkan penyalahgunaan wewenang atau ketidakseragaman dalam penerapan hukum. Oleh karena itu, ketergantungan pada diskresi justru memperkuat argumen bahwa diperlukan pembaruan norma hukum yang lebih spesifik dan komprehensif.

Lebih lanjut, dari aspek pembuktian, kekosongan norma hukum juga berdampak pada kesulitan dalam proses penyidikan. Dalam kasus *deepfake*, pembuktian tidak hanya berkaitan dengan siapa pelaku, tetapi juga bagaimana membuktikan bahwa suatu konten merupakan hasil rekayasa digital. Hal ini membutuhkan kemampuan forensik digital yang tinggi serta standar pembuktian yang jelas. Namun, karena belum adanya pengaturan khusus mengenai *deepfake*, maka pembuktian sering kali hanya mengandalkan pendekatan umum yang tidak selalu mampu mengungkap kompleksitas teknologi yang digunakan. Akibatnya, proses penegakan hukum menjadi tidak optimal dan berpotensi menghambat tercapainya keadilan bagi korban.

Jika dibandingkan dengan penelitian terdahulu, sebagian besar kajian hanya menyoroti kekosongan norma hukum dari sisi regulasi atau dampak sosialnya. Namun, penelitian ini menunjukkan bahwa kekosongan tersebut memiliki implikasi yang lebih luas, yaitu mempengaruhi secara langsung efektivitas penegakan hukum di lapangan. Dengan kata lain, kekosongan norma tidak hanya menjadi masalah teoritis, tetapi juga menjadi hambatan praktis dalam proses penyidikan, penuntutan, dan pembuktian. Temuan ini memperkuat pandangan bahwa pembaruan hukum tidak dapat ditunda, karena keterlambatan dalam merespon perkembangan teknologi akan semakin memperbesar kesenjangan antara hukum dan realitas sosial.

Dalam konteks wilayah Klungkung, fenomena ini memiliki relevansi yang signifikan mengingat meningkatnya penggunaan teknologi digital dalam kehidupan masyarakat. Meskipun belum banyak kasus yang secara eksplisit diklasifikasikan sebagai *deepfake*, potensi penyalahgunaan teknologi ini tetap menjadi ancaman yang nyata. Oleh karena itu, aparat kepolisian perlu memiliki kesiapan tidak hanya dari aspek teknis, tetapi juga dari aspek normatif agar mampu menghadapi perkembangan kejahatan berbasis teknologi secara efektif.

Berdasarkan seluruh analisis tersebut, bahwa konstruksi kekosongan norma hukum dalam penanganan *deepfake* tidak hanya disebabkan oleh ketiadaan aturan, tetapi juga oleh ketidaksesuaian norma yang ada dengan karakteristik kejahatan yang berkembang. Kekosongan ini berdampak pada ketidakpastian hukum, kesulitan pembuktian, serta ketergantungan pada diskresi dalam praktik penegakan hukum. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif dan progresif, khususnya melalui perumusan norma yang secara eksplisit mengatur *deepfake* sebagai bentuk kejahatan siber.

SIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa pengaturan hukum terhadap *deepfake* sebagai alat kejahatan siber di Indonesia masih belum memadai dan belum dirumuskan secara spesifik dalam hukum positif. Ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana memang masih dapat digunakan untuk

menjerat pelaku melalui pendekatan pasal-pasal umum, seperti kesusilaan, pencemaran nama baik, ancaman, dan penyebaran informasi bohong. Namun, penggunaan norma tersebut bersifat tidak langsung dan hanya menjangkau akibat dari penyalahgunaan *deepfake*, bukan mengatur *deepfake* sebagai bentuk kejahatan yang berdiri sendiri. Kondisi ini menunjukkan bahwa hukum masih tertinggal dalam merespons perkembangan teknologi *artificial intelligence*, sehingga menimbulkan ketidakpastian hukum dalam praktik penegakan hukum.

Selanjutnya, konstruksi kekosongan norma hukum dalam penanganan *deepfake* menunjukkan bahwa permasalahan tidak hanya terletak pada ketiadaan aturan, tetapi juga pada ketidaksesuaian norma yang ada dengan karakteristik kejahatan berbasis teknologi digital. Kekosongan tersebut bersifat struktural, yang tercermin dari tidak adanya definisi hukum, tidak adanya rumusan delik khusus, serta belum adanya standar pembuktian yang memadai. Dalam praktik penegakan hukum, kondisi ini berdampak pada penggunaan pendekatan kasuistis oleh aparat kepolisian yang sangat bergantung pada interpretasi dan diskresi. Akibatnya, penegakan hukum menjadi tidak konsisten, sulit dibuktikan, serta berpotensi menghambat perlindungan hukum terhadap korban. Hal ini menunjukkan bahwa sistem hukum masih berada dalam tahap adaptasi dan belum mampu secara optimal menghadapi kejahatan berbasis *deepfake*.

Saran

Berdasarkan kesimpulan tersebut, diperlukan langkah konkret dalam bentuk pembaruan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi digital, khususnya melalui perumusan regulasi yang secara eksplisit mengatur *deepfake* sebagai bentuk kejahatan siber. Selain itu, aparat penegak hukum perlu diperkuat dari aspek kapasitas teknis, terutama dalam bidang forensik digital, agar mampu mengidentifikasi dan membuktikan kejahatan berbasis teknologi secara lebih akurat. Di sisi lain, diperlukan penyusunan pedoman penegakan hukum yang lebih jelas guna mengurangi ketergantungan pada diskresi dan meminimalisir perbedaan penafsiran di lapangan. Dengan demikian, penegakan hukum terhadap *deepfake* dapat berjalan lebih efektif serta mam

DAFTAR PUSTAKA

Buku:

Flora, H. S. (2024). *Hukum pidana di era digital*. Jakarta: Rajawali Pers.

Hiariej, E. O. S. (2022). *Prinsip-prinsip hukum pidana*. Yogyakarta: Cahaya Atma Pustaka.

Hukmana, S. Y. (2025, April 24). *2 tersangka kasus penipuan AI deepfake face Presiden Prabowo segera disidang*. Metro TV News.

Kusnadi, S. A., & Putri, D. W. S. (2025). *Pengantar hukum siber Indonesia*. Jakarta: Kencana.

Prasetyo, T. (2023). *Hukum pidana*. Jakarta: Rajawali Pers.

Rahman, A. (2025). *Pengantar cybercrime dalam sistem hukum pidana Indonesia*. Yogyakarta: Deepublish.

Sihotang, H. (2024). *Hukum cybercrime 4.0: Kejahatan digital dan artificial intelligence*. Bandung: Refika Aditama.

Jurnal:

Arvitto, R. S. (2025). Implikasi hukum *deepfake*: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia, 4*(2), 73–82. https://doi.org/10.35912/jihham.v4i2.3937

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan hukum terhadap penyalahgunaan *deepfake* pada pornografi anak di era *artifical intelegence* di Indonesia. *Jurnal Penelitian Serambi Hukum, 18*(1), 42–54. https://doi.org/10.59582/sh.v18i01.1257

Devi, W. Z. (2026). Implikasi hukum terhadap penyalahgunaan teknologi *deepkfake* untuk pemerasan (*sextortion*) dalam perspektif hukum teknologi informasi di Indonesia. *Majelis: Jurnal Hukum Indonesia, 3*(1), 102–114. https://doi.org/10.62383/majelis.v3i1.1504

Fauzi, S. S., Rusmana, I. P. E., Darma, I. M. W., & Wulandari, N. G. A. A. M. T. (2025). Pengaturan sanksi pidana terhadap pelaku pembuat konten pornografi dengan menggunakan teknologi *deepfake* di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3*(6), 9612–9623. https://doi.org/10.61104/alz.v3i6.2661

Kusnadi, S. A., & Putri, D. W. S. (2025). Perlindungan hak privasi dalam penyalahgunaan teknologi *deepfake* di Indonesia. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional, 14*(2). https://doi.org/10.33331/rechtsvinding.v14i2.2135

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi *deepfake* di Indonesia sebagai bentuk pelindungan negara. *Jurnal USM Law Review, 7*(2), 603–621.

Prayoga, D. K., & Edrisy, I. F. (2025). Urgensi pengaturan hukum terhadap *deepfake* sebagai alat kejahatan siber dalam perspektif KUHP dan UU ITE. *Journal Evidence of Law, 4*(3), 1666–1673. https://doi.org/10.59066/jel.v4i3.1865

Wanggai, F. R. M., Hartono, M. S., & Parwati, N. P. E. (2026). Analisis normatif terhadap penyebaran *deepfake* sebagai bentuk kejahatan siber di Indonesia. *Majelis: Jurnal Hukum Indonesia, 3*(1), 122–130. https://doi.org/10.62383/majelis.v3i1.1509

Peraturan Perundang-undangan:

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.