Volume 13 Nomor 2 September 2026

Jurnal Jendela Hukum

https://www.ejournalwiraraja.com/index.php/FH P-ISSN : 2355-5831, E-ISSN : 2355-9934

PERTANGGUNGJAWABAN PIDANA ATAS KONTEN *DEEPFAKE* DALAM KUHP NASIONAL

Zainur Rohman
Universitas Wiraraja
Email : manunggalputra78@gmail.com

ABSTRACT

The misuse of deepfake technology to imitate a person's face, voice, or actions poses a problem for criminal law, because Indonesia's National Criminal Code (Law Number 1 of 2023), which took effect on 2 January 2026, has no offence that expressly mentions deepfakes. This article asks whether the National Criminal Code can reach the making and spreading of deepfake content, and how criminal liability can be built for individuals and corporations. The study is normative juridical research that uses the statute approach and the conceptual approach. It relies on primary, secondary, and non-legal materials gathered through library research and analysed qualitatively. The results show that deepfakes are covered only in part, and which provision applies depends on the purpose of the conduct: fraud (Article 492), forgery (Article 391), pornography (Article 407), defamation (Article 433), and false news that causes unrest (Articles 263 and 264, as amended by Law Number 1 of 2026). Each of these provisions was drafted with conventional methods in mind, so problems remain around the element of "letter", synthetic content that portrays someone instead of accusing them, the consent of the person portrayed, and negligent sharers. Under the general provisions, individuals are liable if they act intentionally as perpetrators, co-perpetrators, or accessories (Articles 20, 21, and 36), whereas artificial intelligence cannot be a subject of criminal law. Corporations, including platforms and AI service providers, can be held liable under Articles 45 to 48 when the offence is accepted as corporate policy, allowed to happen, or when preventive measures are ignored. Because the principle of legality forbids analogy, an explicit offence on deceptive synthetic content is needed, together with transparency obligations.

Keywords: *Deepfake. Criminal Liability. National Criminal Code*

ABSTRAK

Penyalahgunaan teknologi *deepfake* untuk meniru wajah, suara, atau tindakan seseorang menjadi tantangan bagi hukum pidana, sebab KUHP Nasional (Undang-Undang Nomor 1 Tahun 2023) yang mulai berlaku pada 2 Januari 2026 tidak memiliki delik yang secara tegas menyebut *deepfake*. Tulisan ini mengkaji apakah KUHP Nasional mampu menjangkau perbuatan membuat dan menyebarkan konten *deepfake*, serta bagaimana pertanggungjawaban pidananya disusun untuk orang perseorangan dan korporasi. Penelitian ini tergolong penelitian yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan yang dipakai adalah bahan hukum primer, sekunder, dan nonhukum yang dikumpulkan lewat studi kepustakaan, lalu dianalisis secara kualitatif. Hasilnya menunjukkan bahwa *deepfake* hanya terjangkau sebagian, tergantung tujuan perbuatannya, yaitu penipuan (Pasal 492), pemalsuan surat (Pasal 391), pornografi (Pasal 407), pencemaran (Pasal 433), dan berita bohong yang menimbulkan kerusuhan (Pasal 263 dan 264 sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2026). Semua pasal itu dibuat untuk cara-cara konvensional, sehingga masih ada masalah pada unsur "surat", pada konten sintetis yang menggambarkan seseorang tanpa menuduhnya, pada persetujuan orang yang digambarkan, dan pada penyebar yang lalai. Berdasarkan ketentuan umum, orang perseorangan dapat bertanggung jawab jika dengan sengaja berperan sebagai pelaku, turut serta, atau pembantu (Pasal 20, 21, dan 36), sedangkan kecerdasan buatan tidak dapat menjadi subjek hukum pidana. Korporasi, termasuk platform dan penyedia layanan kecerdasan buatan, dapat dimintai pertanggungjawaban berdasarkan Pasal 45 sampai dengan 48 apabila tindak pidana diterima sebagai kebijakan, dibiarkan, atau langkah pencegahan diabaikan. Karena asas legalitas melarang analogi, diperlukan rumusan delik yang eksplisit tentang konten sintetis yang menyesatkan, dilengkapi kewajiban transparansi.

Kata kunci: *Deepfake*. Pertanggungjawaban Pidana. KUHP Nasional

1. PENDAHULUAN

Perkembangan kecerdasan buatan (*artificial intelligence*) mengubah cara orang membuat dan mempercayai informasi. Salah satu hasilnya yang paling mengkhawatirkan adalah *deepfake*, yaitu media sintetis berupa gambar, suara, atau video yang dibuat dengan teknik pembelajaran mendalam (*deep learning*) untuk menirukan wajah, suara, atau gerak-gerik seseorang sampai terlihat asli. Awalnya teknologi ini dipakai untuk hiburan dan industri kreatif. Sekarang ia juga dipakai untuk menipu dengan menirukan wajah dan suara atasan atau keluarga, membuat konten seksual dengan menempelkan wajah korban ke tubuh orang lain, merusak nama baik tokoh publik, dan menyebarkan disinformasi politik. Korbannya sulit mengenali kejahatan seperti ini, biaya pembuatannya murah, dan penyebarannya bisa melintasi negara hanya dalam hitungan menit. Karena itu hukum pidana harus menjawab dua pertanyaan, yaitu

perbuatan apa yang bisa dipidana, dan siapa yang bertanggung jawab ketika kontennya dibuat oleh sistem otomatis, disebarkan banyak orang, dan ditampung oleh platform.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional) mulai berlaku pada 2 Januari 2026. Di hari yang sama, Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana (UU 1/2026) juga berlaku dan mengubah beberapa ketentuannya.[1] KUHP Nasional tidak menyebut istilah *deepfake*, jadi dasar pemidanaannya harus dicari pada delik-delik yang sudah ada. Pasal 1 ayat (1) menyatakan bahwa seseorang hanya dapat dipidana atas perbuatan yang sudah ditetapkan sebagai tindak pidana oleh peraturan perundang-undangan sebelum perbuatan itu dilakukan, dan ayat (2) melarang penggunaan penafsiran analogi untuk menetapkan suatu tindak pidana.

Delik yang paling mendekati adalah penipuan dalam Pasal 492. Pasal ini memidana orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, memakai nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kata bohong untuk menggerakkan orang lain menyerahkan barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dengan ancaman penjara paling lama empat tahun. Selanjutnya ada pemalsuan surat dalam Pasal 391, yang memidana pembuatan atau pemalsuan surat yang dapat menimbulkan hak, perikatan, atau pembebasan utang, atau yang diperuntukkan sebagai bukti, jika pemakaiannya dapat menimbulkan kerugian, dengan ancaman penjara paling lama enam tahun. Pasal 407 melarang perbuatan memproduksi, membuat, menyebarluaskan, atau menyiarkan pornografi dengan ancaman penjara paling lama sepuluh tahun, tetapi mengecualikan perbuatan untuk kepentingan seni, budaya, olahraga, kesehatan, atau ilmu pengetahuan. Pasal 433 memidana orang yang menyerang kehormatan atau nama baik orang lain dengan menuduhkan suatu hal agar diketahui umum. Ancamannya lebih berat jika dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan, atau ditempelkan di tempat umum, dan ada pengecualian untuk perbuatan demi kepentingan umum atau pembelaan diri.

[1] Dandapala, "Baru berlaku langsung diubah, berikut pasal KUHP baru yang disesuaikan," 2026, https://dandapala.com/article/detail/baru-berlaku-langsung-diubah-berikut-pasal-kuhp-baru-yang-disesuaikan.

Di luar KUHP Nasional, Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE) melarang setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum memanipulasi, menciptakan, mengubah, menghilangkan, atau merusak informasi elektronik dan/atau dokumen elektronik agar dianggap seolah-olah data yang otentik. Pasal 51 ayat (1) mengancamnya dengan penjara paling lama dua belas tahun. Pasal 14 ayat (1) Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS) memidana kekerasan seksual berbasis elektronik, yaitu merekam atau mengambil gambar bermuatan seksual tanpa persetujuan, mengirim muatan seksual kepada penerima yang tidak menghendaki, dan menguntit untuk tujuan seksual, dengan ancaman penjara paling lama empat tahun dan/atau denda paling banyak Rp200.000.000,00. Pasal 66 jo. Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) melarang pembuatan data pribadi palsu atau pemalsuan data pribadi untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan orang lain, dengan ancaman penjara paling lama enam tahun.

Isu hukumnya ada pada ketiadaan norma yang secara tegas mengatur *deepfake*, sementara norma yang bisa dipinjam tersebar di beberapa undang-undang dan semuanya dibuat untuk perbuatan konvensional. Keadaan ini bertabrakan dengan dua pilar teori hukum pidana. Pilar pertama adalah asas legalitas, yang menuntut rumusan delik tertulis (*lex scripta*), jelas (*lex certa*), dan tidak diperluas dengan analogi (*lex stricta*).[2] Padahal kejahatan berbasis teknologi berkembang lebih cepat daripada pembentukan undang-undang, sehingga aparat penegak hukum mudah tergoda memperluas rumusan lama. Pilar kedua adalah asas tiada pidana tanpa kesalahan (*geen straf zonder schuld*), yang menuntut pembuktian kesengajaan atau kealpaan pada pelaku.[3] Padahal konten sintetis dibuat oleh sistem otomatis, disebarkan banyak orang yang bisa jadi tidak tahu kontennya palsu, dan difasilitasi penyedia layanan yang tidak ikut membuat isinya.

[2] Moeljatno, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 2008).
[3] S I P Law Firm, "Konten deepfake dan ancaman pidananya di Indonesia," 2025, https://siplawfirm.id/resources/konten-deepfake.

Pertanggungjawaban pidana berpusat pada manusia dan korporasi, dan kecerdasan buatan bukan subjek hukum pidana.

Berdasarkan uraian di atas, rumusan masalah penelitian ini ada dua. Pertama, bagaimana KUHP Nasional dapat menjangkau perbuatan membuat dan menyebarkan konten *deepfake*, dan di mana letak celah normanya. Kedua, bagaimana pertanggungjawaban pidana atas konten *deepfake* dikonstruksikan bagi orang perseorangan dan korporasi menurut ketentuan umum KUHP Nasional. Tujuan penelitian ini adalah memetakan sejauh mana delik-delik KUHP Nasional menjangkau berbagai bentuk *deepfake*, menyusun konstruksi pertanggungjawaban pidana bagi pembuat, penyebar, pembantu, dan korporasi, serta merumuskan arah pembaruan norma.

Penelitian ini penting karena tiga alasan. Pertama, KUHP Nasional baru saja berlaku, sehingga aparat penegak hukum dan akademisi masih dalam masa peralihan dari rujukan lama. Kementerian Komunikasi dan Digital dilaporkan masih memakai UU ITE dan KUHP untuk menangani kasus *deepfake* karena belum ada undang-undang khusus tentang kecerdasan buatan,[4] sementara peraturan presiden tentang kecerdasan artifisial baru dalam tahap persiapan pada awal 2026.[5] Kedua, ancaman pidana hanya boleh dimuat dalam undang-undang atau peraturan daerah (Pasal 15 ayat (1) Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan), sehingga celah norma pidana tidak bisa ditutup dengan peraturan presiden. Ketiga, korban *deepfake* bisa kehilangan kehormatan, harta, dan kepercayaan publik dengan cepat, dan ketidakpastian norma membuat mereka sulit mendapat keadilan.

Beberapa penelitian terdahulu sudah membahas topik ini. Rijkie meneliti perlindungan hukum bagi korban *deepfake* pornografi berdasarkan UU ITE, KUHP baru, dan UU TPKS. Ia menyimpulkan bahwa ketiganya belum mengatur *deepfake* pornografi secara eksplisit sehingga terjadi kekosongan hukum, dan merekomendasikan regulasi khusus.[6] Kajiannya terbatas pada pornografi dan sudut pandang korban. Ramadan dan

[4] Firm.
[5] ANTARA, "Perpres AI siapkan tata kelola pengembangan teknologi secara etis," 2026, https://megapolitan.antaranews.com/berita/513926/perpres-ai-siapkan-tata-kelola-pengembangan-teknologi-secara-etis.
[6] Z R Rijkie, "Perlindungan Hukum terhadap Korban Deepfake Pornografi dalam Perspektif Hukum Pidana Indonesia," *Jurnal Pendidikan Tambusai* 10, no. 2 (2026), https://doi.org/10.31004/jptam.v10i2.41089.

Wahyudi membandingkan KUHP dan UU ITE untuk menilai urgensi reformulasi sanksi pidana *deepfake*; fokus mereka pada sanksi, dan kajiannya terbit sebelum KUHP Nasional berlaku.[7] Akbar, Yulia, dan Romdoni membahas perlunya reformulasi UU ITE terhadap *deepfake* dengan merujuk pada EU AI Act dan regulasi *deep synthesis* di Tiongkok, sehingga objek pembaruannya adalah UU ITE.[8] Penelitian ini berbeda dalam tiga hal. Pertama, titik awalnya KUHP Nasional yang sudah berlaku beserta perubahannya melalui UU 1/2026. Kedua, yang dikaji bukan hanya delik tertentu atau sanksinya, tetapi konstruksi pertanggungjawaban lewat ketentuan umum Buku Kesatu (Pasal 20, 21, 36, 37, dan 45 sampai dengan 48), termasuk posisi penyebar yang tidak tahu kontennya palsu dan penyedia platform. Ketiga, penelitian ini memetakan semua bentuk *deepfake*, yaitu penipuan, pemalsuan, pornografi, pencemaran, dan disinformasi, bukan hanya satu bentuk.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif. Sifat normatifnya terlihat dari objek kajiannya, yaitu norma hukum positif berupa rumusan delik dan ketentuan umum KUHP Nasional beserta undang-undang lain yang berkaitan, asas-asas hukum pidana yang mendasarinya, serta kekosongan dan ketidakjelasan norma yang ditemukan, tanpa mengumpulkan data perilaku di lapangan.[9] Penelitian ini juga bersifat preskriptif, karena tidak berhenti pada penjelasan norma tetapi juga memberikan argumen tentang bagaimana norma seharusnya dirumuskan. Pendekatan yang dipakai ada dua. Pendekatan perundang-undangan (*statute approach*) dilakukan dengan menelaah KUHP Nasional, UU 1/2026, UU ITE, UU TPKS, dan UU PDP. Pendekatan konseptual (*conceptual approach*) dilakukan dengan menelaah konsep *deepfake*, asas legalitas, asas kesalahan, dan pertanggungjawaban pidana korporasi.

---

[7] M I Ramadan and E Wahyudi, "Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake dalam KUHP dan UU ITE," *Jurnal Hukum Sehasen* 11, no. 2 (2025): 353–62, https://doi.org/10.37676/jhs.v11i2.9463.

[8] B M Akbar, R Yulia, and M Romdoni, "Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana" (Universitas Sultan Ageng Tirtayasa, 2026), https://eprints.untirta.ac.id/57703/.

[9] Peter Mahmud Marzuki, *Penelitian Hukum*, Edisi Revisi (Jakarta: Kencana, 2017).

Bahan hukum primernya adalah peraturan perundang-undangan tersebut. Bahan hukum sekunder terdiri dari buku, artikel jurnal, dan hasil penelitian terdahulu. Bahan nonhukum berupa pemberitaan kantor berita dan situs resmi pemerintah, yang dipakai terbatas untuk melihat perkembangan kebijakan. Semua bahan dikumpulkan melalui studi kepustakaan, yakni menelusuri peraturan dan publikasi ilmiah secara daring, lalu dicatat dan dikelompokkan sesuai rumusan masalah. Karena teks konsolidasi KUHP Nasional setelah UU 1/2026 belum tersedia saat penelitian ini dilakukan, bunyi pasal diambil dari naskah Undang-Undang Nomor 1 Tahun 2023 dan dicocokkan dengan perubahan yang diberitakan. Analisis dilakukan secara kualitatif dengan penafsiran gramatikal dan sistematis, lalu disusun secara deduktif: norma sebagai premis mayor, bentuk-bentuk *deepfake* sebagai premis minor, dan keterjangkauan serta konstruksi pertanggungjawabannya sebagai kesimpulan.

3. HASIL PENELITIAN DAN PEMBAHASAN

Jawaban untuk rumusan masalah pertama dimulai dari satu temuan, yaitu KUHP Nasional tidak memuat delik yang menyebut atau menyasar *deepfake*, sehingga apakah ia terjangkau atau tidak bergantung pada tujuan dan akibat dari konten yang dibuat. Pasal 1 ayat (1) dan ayat (2) menutup jalan pintas berupa penafsiran analogi. Akibatnya, setiap bentuk *deepfake* baru bisa dipidana kalau semua unsur delik yang ada terpenuhi menurut bunyi teksnya. Singkatnya, hukum tidak memidana *deepfake* karena teknologinya, melainkan memidana penipuan, pemalsuan, pornografi, atau pencemaran yang kebetulan dilakukan dengan teknologi itu.

Pada *deepfake* penipuan, misalnya video atau suara sintetis yang meniru direktur untuk memerintahkan transfer dana, Pasal 492 relatif mudah diterapkan. Rumusannya tidak menyebut sarana tertentu, dan unsur nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kata bohong bisa mencakup peniruan identitas dan jabatan lewat media sintetis. Unsur yang menentukan adalah akibatnya: korban harus sudah menyerahkan barang, memberi utang, membuat pengakuan utang, atau menghapus piutang karena tergerak oleh tipu muslihat tersebut. Kalau korban sadar bahwa itu palsu sebelum menyerahkan apa pun, pelaku hanya bisa dipidana berdasarkan ketentuan percobaan

dalam Buku Kesatu, bukan Pasal 492 yang sudah selesai. Jadi persoalan utamanya bukan celah rumusan, melainkan pembuktian bahwa konten sintetis tertentu itulah yang menggerakkan korban, serta pelacakan pelaku yang anonim.

Pemalsuan identitas lewat video verifikasi atau dokumen sintetis lebih bermasalah. Pasal 391 ayat (1) mensyaratkan adanya "surat" yang dapat menimbulkan hak, perikatan, atau pembebasan utang atau yang diperuntukkan sebagai bukti, dan ayat (2) memidana pemakaian surat palsu seolah-olah asli. Apakah gambar atau video sintetis dan dokumen elektronik termasuk "surat" tidak bisa dijawab dari teks pasalnya sendiri. Kalau dijawab dengan tafsir yang luas, ada risiko melanggar larangan analogi dalam Pasal 1 ayat (2). Jalur yang lebih aman adalah Pasal 35 UU ITE, yang tegas menyebut "penciptaan" informasi elektronik agar dianggap seolah-olah data otentik, dengan ancaman penjara paling lama dua belas tahun menurut Pasal 51 ayat (1), dua kali lipat dari ancaman Pasal 391. Namun pasal ini pun tidak bebas masalah. Rumusan "dianggap seolah-olah data yang otentik" paling cocok untuk memalsukan data yang sudah ada, sedangkan *deepfake* sering menciptakan peristiwa yang tidak pernah terjadi, sehingga masih bisa diperdebatkan apakah ia meniru keotentikan suatu data. Ketentuan UU ITE yang perbuatan terlarangnya sudah diatur dalam KUHP Nasional, seperti kesusilaan, penghinaan, dan akses ilegal, dialihkan ke KUHP Nasional, sedangkan Pasal 35 tidak termasuk ketentuan yang dialihkan itu,[10] sehingga pasal tersebut tetap bisa dipandang sebagai norma khusus (*lex specialis*) untuk manipulasi informasi elektronik.

Deepfake seksual, yaitu menempelkan wajah korban pada tubuh orang lain dalam konten seksual, bisa diperiksa lewat dua jalur. Jalur pertama adalah Pasal 407 KUHP Nasional yang memidana setiap orang yang memproduksi, membuat, menyebarluaskan, atau menyiarkan pornografi. Perbuatannya dirumuskan luas, jadi pembuatan dan penyebaran konten sintetis ikut tercakup selama kontennya memenuhi pengertian pornografi. Tetapi delik ini dirumuskan sebagai delik kesusilaan dan tidak menjadikan ketiadaan persetujuan orang yang digambarkan sebagai unsur. Kerugian khas korban, yaitu identitas dan martabatnya dipakai tanpa izin, tidak terlihat dalam rumusannya.

[10] Kementerian Komunikasi dan Digital, "Artikel Hukum: Perubahan Kedua UU ITE," JDIH Komdigi, t.t., https://jdih.komdigi.go.id/artikel_hukum/artikel-hukum/unduh/85.

Selain itu, pengecualian untuk karya seni, budaya, olahraga, kesehatan, atau ilmu pengetahuan pada ayat (2) bisa dipakai pelaku sebagai pembelaan. Jalur kedua adalah Pasal 14 ayat (1) UU TPKS. Huruf a mensyaratkan adanya perekaman atau pengambilan gambar bermuatan seksual tanpa persetujuan, yang mengandaikan ada peristiwa nyata yang direkam, padahal *deepfake* menghasilkan gambar tanpa peristiwa. Huruf b, yakni pengiriman muatan seksual kepada penerima yang tidak menghendaki, bisa menjangkau penyebaran, dan ayat (2) memperberat pidana kalau dilakukan untuk memeras, mengancam, atau memperdaya. Dengan begitu, pembuatan konten seksual sintetis yang belum disebarkan, serta penyebaran ke publik tanpa penerima tertentu, berada di wilayah abu-abu. Temuan ini sejalan dengan kesimpulan Rijkie bahwa ketiga undang-undang belum mengatur *deepfake* pornografi secara eksplisit.[11]

Deepfake yang menampilkan tokoh publik mengatakan atau melakukan sesuatu yang tidak pernah terjadi bisa diperiksa lewat Pasal 433. Ayat (1) memidana penyerangan kehormatan atau nama baik dengan menuduhkan suatu hal agar diketahui umum, dan ayat (2) memperberat pidananya jika dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan, atau ditempelkan di tempat umum. Ada dua masalah di sini. Pertama, delik ini mensyaratkan "menuduhkan suatu hal", sedangkan *deepfake* tidak mengucapkan tuduhan tetapi menampilkan peristiwa seolah-olah nyata, sehingga menyamakan keduanya sudah mendekati perluasan makna. Kedua, ayat (3) mengecualikan perbuatan yang dilakukan demi kepentingan umum atau karena terpaksa membela diri, sehingga satire dan parodi politik berbasis media sintetis akan diperdebatkan di titik ini. Untuk *deepfake* yang dimaksudkan menimbulkan kegaduhan, Pasal 263 dan 264 tentang penyiaran berita bohong yang menimbulkan kerusuhan bisa dipertimbangkan. Akan tetapi UU 1/2026 membatasi pertanggungjawaban dalam kedua pasal itu hanya pada perbuatan yang dilakukan dengan sengaja,[12] sehingga penyebar yang lalai tidak lagi bisa dijangkau.

[11] Rijkie, "Perlindungan Hukum terhadap Korban Deepfake Pornografi dalam Perspektif Hukum Pidana Indonesia."
[12] Dandapala, "Baru berlaku langsung diubah, berikut pasal KUHP baru yang disesuaikan."

UU PDP memberi jalur lain yang jarang dibahas. Wajah dan suara yang dapat mengidentifikasi seseorang termasuk data pribadi, dan data biometrik termasuk data pribadi yang bersifat spesifik (Pasal 4 ayat (2) UU PDP). Pasal 66 jo. Pasal 68 UU PDP memidana pembuatan data pribadi palsu atau pemalsuan data pribadi untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan orang lain, sehingga peniruan wajah atau suara seseorang untuk memperoleh keuntungan bisa dipandang sebagai pembuatan data pribadi palsu. Kelebihannya, UU PDP juga mengatur pertanggungjawaban korporasi secara tegas dalam Pasal 70. Kekurangannya, penafsiran "data pribadi palsu" untuk konten sintetis belum pernah diuji, dan unsur keuntungan menyempitkan jangkauannya pada motif ekonomi atau pribadi, padahal banyak *deepfake* dibuat untuk merundung atau mempermalukan.

Dari pemetaan itu terlihat bahwa KUHP Nasional hanya menjangkau *deepfake* secara parsial dan sangat bergantung pada tujuannya. Penipuan terjangkau dengan baik. Pemalsuan tidak pasti karena unsur "surat". *Deepfake* seksual terjangkau pada tahap penyebaran, tetapi kerugian korban atas identitasnya tidak dikenali oleh rumusan pasal. Pencemaran dibatasi oleh unsur "menuduhkan", dan disinformasi dibatasi pada kesengajaan. Pembuatan *deepfake* yang belum dipakai atau disebarkan hampir tidak terjangkau, kecuali lewat Pasal 407 atau Pasal 35 UU ITE. Fragmentasi ini juga membuat ancaman pidana tidak seragam untuk perbuatan yang pada dasarnya sama, yaitu memalsukan identitas seseorang dengan media sintetis: empat tahun untuk penipuan, enam tahun untuk pemalsuan surat, sepuluh tahun untuk pornografi, dan dua belas tahun untuk manipulasi informasi elektronik. Dari sisi kebijakan hukum pidana, kriminalisasi yang baik menuntut rumusan yang konsisten dan proporsional,[13] dan kondisi ini belum memenuhinya.

Rumusan masalah kedua menanyakan siapa yang bertanggung jawab. Titik tolaknya Pasal 45 KUHP Nasional, yang menetapkan korporasi sebagai subjek tindak pidana di samping orang perseorangan. Sistem kecerdasan buatan, aplikasi pembuat gambar, atau model bahasa tidak termasuk subjek, jadi tidak ada pertanggungjawaban pidana bagi

[13] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2008).

kecerdasan buatan. Sistem itu hanya sarana, dan pertanggungjawaban selalu kembali kepada manusia atau korporasi di belakangnya.

Untuk orang perseorangan, Pasal 20 menentukan bentuk-bentuk pelaku, yaitu orang yang melakukan sendiri, melalui perantara, turut serta melakukan, atau menggerakkan orang lain. Pembuat yang memakai aplikasi *deepfake* untuk menipu adalah pelaku yang bertindak lewat sarana, dan pemakaian aplikasi tidak mengurangi kesalahannya. Pihak yang membagi tugas, misalnya satu orang membuat video dan orang lain menghubungi korban, termasuk turut serta, dan pihak yang menggerakkan orang lain untuk membuat konten itu bisa dipidana sebagai penggerak. Dalam semua bentuk tadi, perbuatannya tetap harus memenuhi unsur delik yang bersangkutan, karena Pasal 20 hanya menentukan siapa yang dipandang sebagai pelaku.

Pasal 36 menetapkan bahwa seseorang hanya dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukan dengan sengaja atau karena kealpaan, dan tindak pidana karena kealpaan hanya dipidana jika ditentukan secara tegas. Akibatnya cukup penting bagi penyebar. Penipuan dalam Pasal 492 dan pencemaran dalam Pasal 433 adalah delik sengaja, sehingga orang yang meneruskan video sintetis karena yakin video itu asli tidak memenuhi unsur kesengajaan, dan tidak ada rumusan kealpaan yang bisa dipakai. Sebaliknya, orang yang tahu kontennya palsu, atau sadar besar kemungkinan kontennya palsu tetapi tetap menyebarkannya, menurut doktrin dapat dikenai kesengajaan sebagai kemungkinan (*dolus eventualis*). Untuk disinformasi, UU 1/2026 malah mempersempit Pasal 263 dan 264 hanya pada perbuatan yang disengaja,[14] sehingga ruang untuk memidana penyebar yang lalai praktis tertutup. Dari sisi asas kesalahan, hasil ini bisa dibenarkan. Namun dari sisi perlindungan korban, ia meninggalkan ruang bagi penyebaran massal tanpa pertanggungjawaban pidana, yang hanya bisa dijawab dengan tanggung jawab perdata atau administratif, misalnya kewajiban menurunkan konten.

Pengembang atau penjual aplikasi pembuat *deepfake* hanya bisa dijerat sebagai pembantu menurut Pasal 21 kalau dengan sengaja memberi kesempatan, sarana,

[14] Dandapala, "Baru berlaku langsung diubah, berikut pasal KUHP baru yang disesuaikan."

keterangan, atau bantuan pada saat tindak pidana dilakukan. Pengembang yang membuat perangkat serbaguna tanpa tahu adanya tindak pidana tertentu tidak memenuhi syarat ini. Sebaliknya, pengembang yang memasarkan fitur yang memang dibuat untuk menghasilkan gambar telanjang dari foto orang lain tanpa persetujuan, atau menjual layanan suara tiruan kepada pihak yang diketahui akan menipu, bisa dikenai pembantuan. Yang membedakan adalah pengetahuan dan sikap batinnya, bukan sifat teknologinya.

Pasal 37 tidak membuka jalan pintas. UU 1/2026 mengubah pasal ini, dan pemberitaan tentang perubahan tersebut menyebut bahwa pemidanaan tanpa memperhatikan kesalahan (*strict liability*) menjadi inti rumusannya, sedangkan naskah aslinya juga memuat pertanggungjawaban atas perbuatan orang lain.[15] Apa pun rincian rumusan akhirnya, pemidanaan tanpa kesalahan dan pertanggungjawaban atas perbuatan orang lain (*vicarious liability*) hanya terbuka kalau undang-undang menentukannya, dan tidak ada delik *deepfake* yang dirumuskan seperti itu. Gagasan agar penyedia platform dibebani pertanggungjawaban pidana atas perbuatan penggunanya karena itu tidak bisa bersandar pada Pasal 37, dan penyedia layanan hanya bisa dijangkau lewat jalur korporasi.

Jalur korporasi memiliki rumusan yang lebih rinci. Pasal 45 mencakup perseroan terbatas, yayasan, koperasi, badan usaha milik negara dan daerah, perkumpulan, firma, persekutuan komanditer, dan bentuk lain yang disamakan. Pasal 46 menentukan bahwa tindak pidana oleh korporasi dilakukan oleh pengurus yang berkedudukan fungsional atau orang yang bertindak untuk dan atas nama korporasi, dan Pasal 47 memperluasnya pada pemberi perintah, pemegang kendali, atau pemilik manfaat yang berada di luar struktur organisasi. Pasal 48 menambahkan syarat bahwa korporasi dapat dimintai pertanggungjawaban jika tindak pidana termasuk lingkup usaha atau kegiatan korporasi, menguntungkan korporasi secara melawan hukum, diterima sebagai kebijakan korporasi, korporasi tidak mengambil langkah yang diperlukan untuk mencegah tindak pidana, mencegah dampak yang lebih besar, dan memastikan kepatuhan hukum,

[15] Ibid.

dan/atau korporasi membiarkan tindak pidana terjadi. Bagi penyedia layanan kecerdasan buatan, tiga syarat terakhir paling relevan. Penyedia yang memasarkan fitur peniruan wajah atau suara tanpa verifikasi persetujuan, tidak menyediakan saringan atau pelabelan padahal tahu risiko penyalahgunaannya, atau membiarkan penyalahgunaan setelah ada laporan, memenuhi gambaran tindak pidana yang diterima sebagai kebijakan, korporasi yang tidak mengambil langkah pencegahan, dan korporasi yang membiarkan. UU 1/2026 menambahkan dalam Pasal 132 ayat (2) bahwa penuntutan korporasi tidak gugur karena kepailitan, perubahan nama, penggabungan, peleburan, pengambilalihan, pemisahan, atau pembubaran,[16] sehingga ruang untuk berkelit lewat restrukturisasi menjadi lebih sempit.

Meski begitu, jalur korporasi punya batas. Pasal 48 mengandaikan adanya tindak pidana yang dilakukan oleh atau untuk korporasi menurut Pasal 46 dan 47. Platform yang hanya menjadi tempat pengguna mengunggah *deepfake* tidak otomatis memenuhi hal itu, karena yang melakukan tindak pidana adalah pengguna, bukan pengurus atau orang yang bertindak untuk korporasi. Pembiaran juga mensyaratkan adanya tindak pidana yang bisa dihubungkan dengan korporasi dan pengetahuan korporasi atasnya. Tanpa kewajiban hukum yang jelas bagi penyedia layanan untuk mencegah, melabeli, atau menurunkan konten sintetis, penuntut sulit menunjukkan bahwa korporasi tidak mengambil langkah yang diperlukan. Karena itu hukum administratif dan perdata perlu lebih dulu merumuskan kewajiban tersebut, sehingga pelanggarannya baru kemudian bisa dibebani pidana.

Ada dua hambatan praktis yang memengaruhi konstruksi ini. Pertama, pembuktian: terdakwa akan mempersoalkan keabsahan alat bukti elektronik dan keandalan alat deteksi *deepfake*, sehingga penuntut membutuhkan dukungan forensik digital yang terstandar. Kedua, yurisdiksi: Pasal 4 huruf c memperluas berlakunya ketentuan pidana Indonesia terhadap tindak pidana di bidang teknologi informasi yang akibatnya dialami di wilayah Indonesia, sehingga pembuat yang berada di luar negeri secara normatif tetap bisa dijangkau, walaupun penegakannya bergantung pada kerja sama internasional.

[16] Ibid.

Berdasarkan temuan tersebut, perlu dirumuskan norma tersendiri yang memuat empat hal. Pertama, delik inti yang memidana pembuatan atau penyebaran konten sintetis yang realistis atas orang yang dapat diidentifikasi tanpa persetujuannya, dengan maksud menipu, mempermalukan, memeras, atau merugikan, disertai pemberatan untuk muatan seksual, penipuan, dan kepentingan pemilihan umum. Persetujuan dan kerugian orang yang digambarkan harus menjadi pusat rumusan, bukan kesusilaan umum. Kedua, pengecualian yang jelas untuk karya jurnalistik, satire, dan ilmu pengetahuan yang disertai pelabelan, supaya kebebasan berekspresi tetap terlindungi. Ketiga, kewajiban hukum bagi penyedia layanan untuk melabeli, menyaring, dan menurunkan konten, yang kemudian menjadi dasar pemidanaan korporasi menurut Pasal 48. Keempat, norma tersebut ditempatkan dalam undang-undang, karena ketentuan pidana tidak bisa dimuat dalam peraturan presiden (Pasal 15 ayat (1) Undang-Undang Nomor 12 Tahun 2011); peraturan presiden tentang kecerdasan artifisial yang sedang disiapkan hanya dapat mengatur kewajiban administratif.[17] Pendekatan Uni Eropa lewat EU AI Act dan Tiongkok lewat regulasi *deep synthesis*, yang menekankan transparansi dan pelabelan konten sintetis,[18] bisa menjadi bahan perbandingan untuk perumusan itu.

4. KESIMPULAN

Pertama, KUHP Nasional tidak mengatur *deepfake* secara eksplisit dan hanya menjangkaunya sebagian lewat delik penipuan (Pasal 492), pemalsuan surat (Pasal 391), pornografi (Pasal 407), pencemaran (Pasal 433), serta berita bohong yang menimbulkan kerusuhan (Pasal 263 dan 264). Seberapa jauh jangkauannya bergantung pada tujuan dan akibat kontennya, dengan celah pada unsur "surat", unsur "menuduhkan", tidak adanya unsur persetujuan, dan pembuatan konten yang belum disebarkan. Kedua, pertanggungjawaban pidana atas *deepfake* dikonstruksikan lewat ketentuan umum. Orang perseorangan bertanggung jawab sebagai pelaku, turut serta, penggerak, atau pembantu dengan kesengajaan sebagai syarat utama (Pasal 20, 21, dan 36), kecerdasan

[17] ANTARA, "Perpres AI siapkan tata kelola pengembangan teknologi secara etis."
[18] Akbar, Yulia, and Romdoni, "Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana."

buatan bukan subjek hukum pidana, dan korporasi, termasuk platform dan penyedia layanan kecerdasan buatan, dapat dimintai pertanggungjawaban lewat Pasal 45 sampai dengan 48, dengan batas bahwa belum ada kewajiban hukum untuk mencegah dan melabeli konten sintetis. Pembentuk undang-undang disarankan merumuskan delik *deepfake* yang eksplisit dengan persetujuan dan kerugian orang yang digambarkan sebagai pusat rumusan, sedangkan penegak hukum disarankan tidak memperluas Pasal 391, Pasal 433, atau Pasal 407 secara analogis selama norma itu belum ada.

5. DAFTAR PUSTAKA

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

Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan, sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 13 Tahun 2022.

Akbar, B M, R Yulia, and M Romdoni. "Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana." Universitas Sultan Ageng Tirtayasa, 2026. https://eprints.untirta.ac.id/57703/.

ANTARA. "Perpres AI siapkan tata kelola pengembangan teknologi secara etis," 2026. https://megapolitan.antaranews.com/berita/513926/perpres-ai-siapkan-tata-kelola-pengembangan-teknologi-secara-etis.

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2008.

Dandapala. "Baru berlaku langsung diubah, berikut pasal KUHP baru yang disesuaikan," 2026. https://dandapala.com/article/detail/baru-berlaku-langsung-diubah-berikut-pasal-kuhp-baru-yang-disesuaikan.

Firm, S I P Law. "Konten deepfake dan ancaman pidananya di Indonesia," 2025. https://siplawfirm.id/resources/konten-deepfake.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana, 2017.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2008.

Ramadan, M I, and E Wahyudi. "Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake dalam KUHP dan UU ITE." *Jurnal Hukum Sehasen* 11, no. 2 (2025): 353–62. https://doi.org/10.37676/jhs.v11i2.9463.

Rijkie, Z R. "Perlindungan Hukum terhadap Korban Deepfake Pornografi dalam Perspektif Hukum Pidana Indonesia." *Jurnal Pendidikan Tambusai* 10, no. 2 (2026). https://doi.org/10.31004/jptam.v10i2.41089.