Volume 12 Issue 1, 2026
P-ISSN: 2442-8019, E-ISSN: 2620-9837

KEBIJAKAN FORMULASI TINDAK PIDANA DEEPFAKE DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE) DAN UNDANG-UNDANG PELINDUNGAN DATA PRIBADI (UU PDP) DI INDONESIA

Nurul Aulia Fitriani[1], Endik Wahyudi[2]

[1] Faculty of Law, Universitas Esa Unggul, Indonesia.
[2] Faculty of Law, Universitas Esa Unggul, Indonesia.

Abstract: *The development of deepfake technology derived from intelligent computational systems poses a new threat in cybercrime through the manipulation of digital identities whose characteristics closely resemble genuine materials. This study examines the policy formulation of deepfake criminal acts in the current and future Indonesian ITE Law and PDP Law. The research uses the legal protection theory from Philipus M. Hadjon and the criminal law policy theory from Barda Nawawi Arief, with a doctrinal legal analysis emphasizing legislative instruments The results show that the current policy formulation is still implicit and partial, where Article 27 of the ITE Law and Article 65 of the PDP Law can be applied but do not explicitly regulate deepfake as a distinct offense, causing difficulties in evidence and coordination obstacles between institutions. The study concludes that a reformulation is needed through the formulation of a specific deepfake crime with comprehensive elements, adopting the practices of South Korea and China to provide legal certainty and effective victim protection.*

Keywords: *Artificial Intelligence; Deepfake; Policy Formulation.*

How to Site: Nurul Aulia Fitriani, Endik Wahyudi (2026). Kebijakan Formulasi Tindak Pidana *Deepfake* Dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) Di Indonesia. Jurnal hukum to-ra, 12 (1), pp 157-169. DOI 10.55809/tora.v12i1.647

Introduction

Kemajuan teknologi informasi dan komunikasi sudah memicu timbulnya beragam inovasi yang didasarkan pada *Artificial Intelligence* (AI), salah satunya teknologi *deepfake*. Teknologi ini memungkinkan manipulasi visual dan audio seseroang dengan tingkat relaisme tinggi, sehingga berpotensi digunakan untuk kepentingan positif maupun negatif. Di sisi positif, teknologi *deepfake* dapat dimanfaatkan pada sektor kreativitas, ranah pembelajaran, serta bidang lain simulasi digital. Namun di sisi negatif, teknologi *deepfake* ini kerap disalahgunakan untuk penyebaran informasi palsu, pencemaran nama baik, penipuan daring, bahkan eksploitasi seksual. Penerapan AI dalam *cybercrime* termasuk dalam kategori kejahatan berbasis komputer (*computer-related crime*). (Shahzad et al., 2022)

Deepfake merupakan salah satu aspek *Artificial Intelligence* (AI). Dari segi etimologi, istilah "*deepfake*" pada bahasa Inggris merupakan kombinasi dari kata "*deep learning*" yaitu pengembangan komputer untuk berpikir dengan cara meniru kerja otak manusia dan "*fake*" yaitu konten yang dibuat sengaja untuk memanipulasi media yang tampak realistis. Sebagai bagian dari kecerdasan buatan, teknologi *deepfake* memiliki kemampuan untuk memanipulasi fitur wajah individu dengan memanfaatkan kemajuan dalam teknologi AI. (Syahirah et al., 2025) Berdasarkan pengertian tersebut, teknologi ini mampu menciptakan gambar atau rekaman yang menampilkan seseorang melakukan sesuatu yang sebenarnya tidak pernah dilakukannya, melalui pertukaran wajah orang tersebut dengan wajah individu lain dalam media visual. Kemajuan teknologi ini berpotensi membawa akibat buruk, seperti tindak kriminal siber yang dapat menipu masyarakat agar mempercayai berita bohong, serta menghadirkan bahaya yang signifikan karena kemampuannya dalam menyebarkan disinformasi secara luas dan berpotensi memengaruhi pandangan umum. (Juefei-Xu et al., 2022)

Fenomena penyalahgunaan teknologi *deepfake* menunjukkan adanya ancaman baru dalam ranah kejahatan digital (*cybercrime*). Kasus penyebaran video manipulatif yang menyerupai tokoh publik seperti Presiden Joko Widodo atau figur selebritas yaitu Melanie Ricardo yang mempromosikan produk penurun berat badan, menunjukkan betapa mudahnya opini publik dapat digiring oleh konten palsu berbasis AI. Ancaman ini menimbulkan kekhawatiran serius terhadap keamanan data pribadi dan integritas informasi di ruang digital Indonesia.

Menjadi negara yang berlandaskan hukum, Indonesia seharusnya mempunyai peraturan yang mengatur Kecerdasan Buatan (AI), mengingat perkembangannya yang pesat. Secara normatif, Indonesia sudah memiliki dua instrumen hukum yang relevan, yaitu Regulasi Perlindungan Data Pribadi Tahun 2022 bersama ketentuan Informasi dan Transaksi Elektronik Tahun 2008 yang telah mengalami revisi melalui Undang-Undang Tahun 2024, meskipun demikian keduanya tersebut tidak secara eksplisit mengatur penyalahgunaan teknologi *deepfake*. Ketidaksesuaian normatif yang diatur dan kemungkinan adanya perbedaan kewenangan dalam relasi antara dua regulasi tersebut memunculkan tantangan dalam hal efektivitas serta koordinasi pelaksanaan hukum.

Mengacu pada pemaparan sebelumnya, fokus permasalahan penelitian ini dirumuskan Bagaimanakah kebijakan formulasi tindak pidana *deepfake* dalam Undang – Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang – Undang Perlindungan Data Pribadi (UU PDP) di Indonesia saat ini; Bagaimanakah kebijakan formulasi tindak pidana *deepfake* dalam Undang – Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang – Undang Perlindungan Data Pribadi (UU PDP) di Indonesia yang akan datang.

Penelitian ini menerapkan metode normatif yang memfokuskan pada sistem norma sebagai subjek penelitian dengan menerapkan pendekatan peraturan perundang – undangan.(Zainuddin & Dinda Karina, 2023) Landasan hukum penelitian ini bersandar pada sumber primer dan sekunder yang meliputi Sumber hukum utama dalam penelitian ini meliputi regulasi perubahan kedua UU ITE Tahun 2024 serta UU Perlindungan Data Pribadi Tahun 2022. Bahan hukum sekunder mencakup studi kepustakaan yang relevan diambil dari beberapa buku, jurnal hukum dan juga melalui pandangan para ahli.

Metode pengolahan bahan hukum diterapkan melalui pendekatan kualitatif dengan menjabarkan pola dan kebijakan hukum yang berhubungan dengan penelitian yaitu mengenai kebijakan untuk mengatasi penyalahgunaan *deepfake* dalam kejahatan digital, serta menggunakan pendekatan deskriptif preskriptif yang dapat memberikan saran atau rekomendasi mengenai apa yang seharusnya dilakukan untuk mengatasi penyalahgunaan *deepfake* dalam kejahatan digital.

Discussion

Ketentuan dalam UU ITE yang Relevan dengan Tindak Pidana Deepfake

Regulasi hasil perubahan kedua UU ITE Tahun 2024 berfungsi sebagai perangkat hukum utama yang dapat digunakan untuk menjerat pelaku penyalahgunaan teknologi *deepfake* di Indonesia. Meskipun UU ITE tidak secara eksplisit menyebutkan istilah "*deepfake*", pasal dalam undang - undang ini dapat diterapkan untuk menangani berbagai bentuk kejahatan yang memanfaatkan teknologi manipulasi konten digital.

Berdasarkan ketentuan yang tercantum dalam Pasal 27 ayat (3) Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elekronik, yang secara eksplisit menyatakan bahwa *"Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik."* ketentuan pidana ini diatur pada pasal 45 ayat (1) yaitu *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."*

Pasal ini relevan untuk kasus penipuan menggunakan *deepfake* yang mengatasnamakan Mantan Presiden Joko Widodo yang dimana dalam video tersebut dimanipulasi seakan – akan beliau berpidato dengan bahasa china dan kasus *deepfake* yang dialami figur selebritas yaitu Melanie Ricardo Ricardo yang mempromosikan produk penurun berat badan, yang mengakibatkan kerugian ataupun pencemaran nama baik bagi korban.

Lalu sebagaimana diatur pada Pasal 27 ayat (1) UU ITE 2008, Dimana menegaskan bahwa *"Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum."* ketentuan pidana pasal ini juga diatur dalam pasal 45 ayat (1) UU ITE yang berupa pidana penjara paling lama 6 (enam) dan/atau denda maksimal 1 (satu) miliar. Namun, pasal ini memiliki keterbatasan karena hanya berfokus pada aspek penyebaran konten yang bersofat asusila tanpa secara spesifik mengatur mengenai manipulasi menggunkan teknologi AI.

Meskipun dari kedua ketentuan pasal dalam UU ITE Tahun 2008 ini dapat menjerat pelaku *deepfake*, terdapat kelemahan dalam menghadapi fenomena AI yang digunakan secara mendasar yaitu, tidak adanya pengaturan eksplisit tentang *deepfake* sebagai suatu tindak pidana tersendiri, yang menimbulkan tantangan dalam pembuktian unsur delik terutama dalam pembuktian bahwa konten yang disebarkan adalah hasil

manipulasi teknologi AI dan bukan merupakan konten asli.(Koos et al., 2025) Lalu tidak ada ketentuan khusus mengenai kewajiban transparansi atau pelabelan konten yang dihasilkan oleh AI, hal ini berbeda dengan regulasi di negara lain seperti Uni Eropa dan China yang mewajibkan adanya pelabelan konten *AI – generated*.

Ketentuan dalam UU PDP yang Relevan dengan Tindak Pidana Deepfake

UU PDP Tahun 2022 menjamin pengamanan atas informasi pribadi termasuk data biometrik yang sering dimanipulasi dalam teknologi *deepfake*. Berdasarkan ketentuan Pasal 4 UU PDP Tahun 2022 mengklasifikasikan data pribadi menjadi data pribadi yang bersifat umum dan juga yang bersifat spesifik. Data pribadi yang bersifat umum dapat berupa jenis kelamin, agama, kewarganegaraan, nama lengkap, kondisi pernikahan serta informasi pribadi hasil penggabungan untuk mengidentifikasikan seseorang. (Wahyudi et al., n.d.) Lalu data pribadi yang bersifat spesifik meliputi salah satunya pada huruf b yaitu ”data biometrik”. Dalam pasal 4 ayat (2) ini menyatakan bahwa yang dimaksud dengan data biometrik adalah data pribadi yang diperoleh melalui pengukuran atau analisis karakteristik fisik, seperti sidik jari, geometri wajah, iris mata, retina mata, DNA, bentuk telapak tangan, pembuluh darah telapak tangan, suara, dan pola tanda tangan. (Firdausi et al., 2025)

Berdasarkan ketentuan yang tercantum dalam Pasal 65 ayat (1) Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang *menyatakan ”Setiap Orang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.”* dalam konteks *deepfake*, pelaku yang mengambil foto ataupun video seseorang dari media sosial atau sumber lain tanpa adanya izin untuk dijadikan bahan konten *deepfake* dapat dijerat dengan ketentuan ini. Selanjutnya pasal 65 ayat (2) yang menyatakan *”Setiap Orang dilarang secara melawan hukum mengungkapan Data Pribadi yang bukan miliknya”*. Ketentuan ini relevan ketika pelaku *deepfake* membagikan atau mempublikasikan hasil manipulasi yang menggunakan data biometrik korban. Lalu pasal 65 ayat (3) yang menyatakan *”Setiap Orang dilarang secara melawan hukum mengungkapan Data Pribadi yang bukan miliknya.”* Pasal ini secara langsung melarang penggunaan data biometric seseorang untuk membuat konten *deepfake* tanpa adanya persetujuan yang sah.

Ketentuan pidana dari pasal 65 ayat (1), ayat (2), dan ayat (3) ini diatur padal pasal 67 dengan ancaman dengan ancama pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar untuk pelanggaran Pasal 65 ayat (1), lalu pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4 miliar untuk pelanggaran Pasal 65 ayat

(2), selanjutnya pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar untuk pelanggaran Pasal 65 ayat (3).

Undang – Undang Perlindungan Data Pribadi (UU PDP) memberikan perlindungan yang cukup komprehensif dibandingkan dengan Undang – Undang Informasi dan Transkasi Elektronik (UU ITE) dalam konteks *deepfake*, karena UU PDP mengakui data biometrik sebagai data pribadi yang dijelaskan secara spesifik, hal ini sejalan dengan karakteristik teknologi *deepfake* yang pada dasarnya memanipulasi data biometrik seseorang. Lalu UU PDP juga tidak hanya mengatur mengenai penyebarannya, tetapi juga mengenai perolehan dan penggunaan data pribadi tanpa hak dan sanksi yang terdapat pada UU PDP relatif berat dengan adanya tingkat bahaya yang timbul oleh penyalahgunaan teknologi *deepfake*. (Rohmati et al., 2024) Namun UU PDP juga memiliki keterbatasan yaitu, UU PDP tidak secara spesifik menyebutkan teknologi *deepfake* atau *AI-generated content*, sehingga masih memerlukan interpretasi hukum dalam penerapannya.

Koordinasi dan Intergrasi antara UU ITE dan UU PDP

Pada praktik penegakan hukum, kasus *deepfake* dapat dijerat dengan menggunakan kedua undang-undang secara bersamaan *(concursus idealis atau concursus realis)*, tergantung pada unsur-unsur perbuatan yang dilakukan pelaku. Sebagai contoh, dalam kasus *deepfake* pornografi yang disebarkan di media sosial, pelaku dapat dijerat dengan Pasal 27 ayat (1) jo. Pasal 45 ayat (1) UU ITE untuk penyebaran konten asusila dan Pasal 65 ayat (3) jo. Pasal 67 huruf c UU PDP untuk penggunaan data biometrik tanpa hak.

Kedua undang – undang ini merupakan payung hukum dalam penggunaan media teknologi informasi, tetapi dalam pelaksanaanya undang – undang ini belum sepenuhnya mampu menjangkau kejahatan dan pelanggaran yang timbul akibat kemajuan teknologi informasi. (Sengi, 2018)

Meskipun demikian, upaya koordinasi antara kedua undang – undang ini masih dihadapkan pada sejumlah hambatan yaitu, tidak ada pedoman yang eksplisit tentang urutan prioritas atau hierarki dalam penerapan kedua undang – undang tersebut pada kasus *deepfake*. Kondisi ini berpotensi menciptakan ketidakpastian hukum bagi aparat penegak hukum saat memutuskan pasal mana yang harus diutamakan atau cara mengintegrasikan keduanya. Selanjutnya, lembaga yang memiliki kewenangan dalam penegakan hukum berbeda. UU ITE berada di bawah yurisdiksi Kementerian Komunikasi dan Informatika serta aparat penegak hukum tradisional, sedangkan UU PDP mewajibkan pembentukan lembaga khusus bernama Lembaga Pelindungan Data Pribadi, yang hingga kini masih dalam tahap pembentukan. Lalu, prosedur koordinasi antarlembaga terkait, seperti Kementerian Komunikasi dan Informatika, Kepolisian,

Kejaksaan, serta Lembaga Pelindungan Data Pribadi yang akan didirikan, belum diatur secara mendetail. (Penipuan et al., n.d.)

Kebijakan Formulasi Tindak Pidana Deepfake dalam UU ITE dan UU PDP di Indonesia yang Akan Datang

Urgensi Reformulasi Kebijakan Hukum Pidana

Istilah kebijakan hukum pidana dapat pula disebutkan sebagai politik hukum pidana *(penal policy)*. Menurut Prof. Sudarto, melaksanakan ”politik hukum pidana” berarti melakukan pemilihan secara hati – hati untuk mencapai hasil undang – undang pidana yang paling optimal, yaitu yang memenuhi persyaratan keadilan dan efektivitas dalam penggunaanya. Beliau juga mengatakan bahwa pelaksanaan ”politik hukum pidana” merupakan upaya sistematis untuk mewujudkan peraturan undang – undang pidana yang disesuaikan dengan kondisi situasi saat ini, waktu tertentu, serta kebutuhan masa depan. (Prof. Dr. Barda Nawawi Arief, 2008)

Secara konseptual, pembaruan hukum pidana di Indonesia merupakan upaya penataan ulang sistem pemidanaan yang berlandaskan nilai politik, filsafat sosial, dan budaya nasional sebagai fondasi kebijakan sosial, kebijakan kriminal, dan penegakan hukum, yang tidak dapat dilepaskan dari orientasi kebijakan hukum pidana berbasis nilai hukum pidana tidak terlepas dari pendekatan nilai. (Dr. Ismiyanto et al., 2025)

Perkembangan teknologi *artificial intelligence* (AI), terkhususnya teknologi *deepfake* yang telah mengubah secara fundamental pola, karakter, dan dampak kejahaan di tuang keamanan siber. Kejahatan tidak lagi dilakukan secara konvensional, melainkan melalui manipulasi identitas digital, wajah, suara, dan citra seseorang secara sangat realistis sehingga sulit untuk dibedakan dari konten autentik. Hal ini menimbulkan tantangan baru bagi hukum pidana, yang pada dasarnya dibangun melalui asumsi perbuatan manusia yang bersifat fisik dan kasat mata. (Prayoga & Tuasikal, 2025) Urgensi reformulasi kebijakan hukum pidana terhadap *deepfake* sebagaimana telah diuraikan sebelumnya menuntut adanya arah kebijakan yang jelas dan terstruktur.

Arah Kebijakan Formulasi Tindak Pidana Deepfake terhadap Masa yang Akan Datang

Kebijakan formulasi tindak pidana *deepfake* di masa mendatang tidak dapat lagi bertumpu pada pendekatan parsial dan sektoral, melainkan harus disusun secara komprehensif dengan mempertimbangkan karakteristik teknologi kecerdasan buatan, perlindungan hak asasi manusia, serta kepastian hukum. Dalam prespektif kebijakan hukum pidana yang sebagiamana dikemukankan oleh Prof. Barda Nawawi Arief yaitu pembaruan hukum pidana harus diarahkan pada upaya perlindungan masyarakat dan

perlindungan korban dengan tetap memperhatikan asas kepastian hukum dan proporsionalitas dalam pemidanaan. (Prof. Dr. Barda Nawawi Arief, 2012)

Keberadaan tahap formulasi ini menunjukkan bahwa upaya – upaya pencegahan dan penanggulangan kejahatan juga merupakan tugas serta kewajiban yang harus diemban oleh para pembuat hukum, bukan hanya menjadi tanggung jawab aparat penegak atau penerap hukum. (Wahyudi & Joe, 2020) Arah kebijakan formulasi yang fundamental adalah diperlukannya perumusan delik khusus *deepfake* dalam peraturan perundang – undangan Indonesia. Delik khusus ini dimaksudkan untuk memberikan kepastian hukum atas perbuatan pembuatan, penyebaran, dan pemanfaatan konten *deepfake* yang dilakukan dengan maksud yang dapat menimbulkan kerugian bagi individu maupun kepentingan publik. Pembentukan delik pidana khusus untuk *deepfake* sangat diperlukan, karena sifat kejahatannya berbeda dari kejahatan siber biasa. *Deepfake* tidak sekadar memanipulasi informasi elektronik, melainkan juga menyalahgunakan identitas, data biometrik, serta kepercayaan masyarakat terhadap konten digital.

Delik khusus *deepfake* idealnya dirumuskan dengan memuat unsur – unsur yang mencermikan karakteristik khas kejahatan berbasis kecerdasan buatan. Unsur perbuatan dalam delik ini mencakup setiap tindakan pembuatan, manipulasi, pemanfaatan, atau penyebaran konten berbasis *artificial intelligence* yang secara teknis mampu merakayasa representasi visual, audio, maupun audiovisual seseorang. Perbuatan tersebut tidak hanya terbatas pada tahap produksi konten *deepfake*, tetapi juga mencakup setiap bentuk pemanfaatan dan distribusi konten kepada publik, baik melalui media sosial dan platform digital.

Lalu unsur objek dalam delik *deepfake* adalah identitas seseorang, yang merupakan data biometrik yang meliputi wajah, suara, ekspresi yang melekat secara personal pada individu tertentu. Identitas merupaka bagian dari hak kepribadian dan hak atas data pribadi yang dilindungi oleh hukum, sehingga setiap bentuk manipulasi atau penggunaan tanpa hak terhadap identitas tersebut dapat dikualifikasikan sebagai pelanggaran terhadap hak manusia. Dengan menempatkan identitas sebagai objek delik, rumusan tindak pidana *deepfake* secara tegas mengakui bahwa penyalahgunaan teknologi AI tidak hanya merugikan secara teknis, namun juga menyerang martabat serta integritas individu.

Selanjutnya, unsur sifat melawan hukum dalam delik *deepfake* ditentukan oleh adanya penggunaan identitas terserbut tanpa persetujuan sah dari subjek ataupun dilakukan dengan tujuan yang dapat merugikan. Persetujuan subjek data harus menjadi tolak ukur utaa dalam menentukan legalitas penggunaan teknologi AI, khususnya ketian menyangkut data biometrik. Oleh karena itu penggunaan teknologi *deepfake* untuk

kepentingan yang menyesatkan, merugikan, atau mengeksploitasi indivdu, baik secara ekonomi, reputasi, hingga psikologis, harus dikualifikasikan sebagai perbuatan melawan hukum.

Unsur terakhir adalah akibat, yaitu dimana timbulnya kerugian sebagai dampak dari perbuatan *deepfake* tersebut. Kerugian yang dimaksud tidak hanya terbatas pada kerugian materiil, tetapi juga mencakup kerugian immaterii; yang berupa pencemaran nama biak, penderitaan psikologis, serta rusaknya reputasi korban. Penyebaran konten *deepfake* juga menimbulkan gangguan terhadap ketertiban umum dan kepentigan publik, seperti penyebaran disinformasi, manipulasi opini publik, serta ancaman terhadap stabilitas sosial. Maka dengan ni perumusan unsur akibat dalam delik *deepfake* menjadi penting untuk menegaskan tingkat bahya kejahatan ini serta sebagai dasar penentuan sanksi pidana yang proporsional.

Perumusan delik khusus ini dapat dilakukan melalui revisi peraturan perundang - undangan dengan menambahkan ketentuan khusus mengenai penyalahgunaan AI, atau melalui pembentukan undang-undang khusus yang mengatur kecerdasan buatan. Pendekatan ini sejalan dengan pandangan Barda Nawawi Arief yang menekankan bahwa kriminalisasi harus dilakukan secara selektif terhadap perbuatan yang benar-benar berbahaya dan meresahkan masyarakat.

Kajian Perbandingan Negara Terhadap Kebijakan Hukum *Deepfake*

Beberapa negara telah menunjukan langkah proaktif terhadap penyalahgunaan *deepfake* yang dapat dijadikan pokok – pokok pikiran yang dapat menjadi acuan terhadap pembentukan regulasi tindak pidana penyalahgunaan *deepfake*. Di Korea Selatan memilih jalur pemidanaan langsung atas *deepfake* seksual non-konsensual dengan merevisi peraturan perundang – undangan kejahatan seksual tahun 2024 – 2025 menegaskan bahwa pembuatan, distribusi, bahkan kepemilikian atau menonton *deepfake* seksual tanpa persetujuan merupakan tindak pidana, dengan ancaman pidana kurungan dan/atau denda yang signifikan. Kebijakan ini dibuat, karena melonjaknya kasus dan dampak korban terutama terhadap perempuan dan remaja, sehingga dibutuhkan penegak untuk pengahpusan cepat konten ilegal dan layanan dukungan korban. Lalu di Tiongkok juga mengatur *deepfake* secara spesifik melalui "*Administrative Provisions on Deep Synthesis in Internet-Based Information Services*" yang merupakan peraturan administratif nasional Tiongkok yang mulai berlaku pada tahun 2023, dengan aturan ini mewajibkan penyedia layanan "sintesis mendalam" (*deep synthesis*) untuk menandai konten sintetis, memastikan keamanan algoritma, serta memnuhi kewajiban *filling*. Larangan berfokus pada penyediaan layanan yang menyesatkan, mengancam ketertiban publik, ataupun melangggar hak subjek data/identitas. (Iradat et al., 2025)

Melalui regulasi – regulasi dari beberapa negara yang secara khusus diatur mengenai penyalahgunaan *deepfake*, dapat disimpulkan bahwa di Indonesia sendiri, memerukan regulasi yang secara eskplisit mengatur mengenai penyalahgunaan *deepfake* sebab menjadi keperluan yang mendesak untuk memastikan jaminan yuridis serta pemerataan keadilan. Dalam hukum pidana Indonesia, pendekatan delik formil di KUHP menyulitkan pengkategorian distribusi konten *deepfake* sebagai tindak pidana, terutama jika platformnya berbasis server luar negeri yang sulit dijangkau yurisdiksi nasional.

Oleh karena itu, regulasi khusus penyalahgunaan *deepfake* akan berdampak besar, karena menawarkan perlindungan tegas bagi individu dari kerusakan reputasi dan pelanggaran privasi. Aturan eksplisit ini memungkinkan negara mengatasi penyebaran konten manipulatif yang mengganggu stabilitas sosial, mengurangi disinformasi, serta menyediakan kepastian hukum bagi korban maupun pelaku, sekaligus memperkuat keandalan sistem informasi digital. Regulasi tersebut juga akan meningkatkan efektivitas penegakan hukum, mendorong pengembangan teknologi yang bertanggung jawab, dan membentuk ekosistem digital yang aman serta transparan. Karenanya, pembentukan delik pidana spesifik untuk *deepfake* menjadi prioritas mendesak, agar hukum nasional selaras dengan kemajuan teknologi, menjaga keamanan siber, serta memastikan hak korban terlindungi secara adil dalam mekanisme peradilan pidana Indonesia.

Conclusion

Kebijakan formulasi tindak pidana *deepfake* dalam UU ITE dan UU PDP di Indonesia saat ini belum memadai karena kedua undang-undang tersebut belum mengatur *deepfake* secara eksplisit sebagai delik pidana tersendiri. UU ITE masih bersifat umum dan hanya menjerat akibat perbuatan berupa penyebaran konten bermuatan pencemaran nama baik atau kesusilaan, sementara UU PDP lebih fokus pada perlindungan data biometrik tanpa menyebut secara langsung teknologi *deepfake*. Kondisi ini menimbulkan kelemahan dalam kepastian hukum, kesulitan pembuktian unsur delik berbasis AI, serta potensi irisan kewenangan antara institusi penegakan hukum dalam penanganan perkara *deepfake*. Lalu, perumusan kebijakan kriminalisasi *deepfake* di masa yang akan datang harus diarahkan pada pembentukan delik khusus yang secara tegas mengatur penyalahgunaan teknologi AI. Delik tersebut perlu memuat unsur perbuatan, objek berupa identitas atau data biometrik, sifat melawan hukum tanpa persetujuan sah atau dengan tujuan merugikan, serta akibat berupa kerugian materiil dan immateriil. Reformulasi ini penting untuk memberikan kepastian hukum, perlindungan efektif bagi korban, serta meningkatkan daya tangkal hukum pidana terhadap kejahatan digital berbasis kecerdasan buatan yang semakin kompleks dan berdampak luas.

Acknowledge

Pertama, pembentuk undang-undang perlu segera melakukan harmonisasi dan penguatan regulasi antara UU ITE dan UU PDP dengan menambahkan ketentuan khusus mengenai penyalahgunaan teknologi *deepfake*. Pemerintah dan DPR disarankan untuk memasukkan delik pidana *deepfake* secara eksplisit melalui revisi undang – undang atau pembentukan regulasi khusus kecerdasan buatan, serta menyusun pedoman penerapan pasal agar aparat penegak hukum memiliki arah yang jelas dan seragam dalam penanganan perkara *deepfake*. Kedua, pemerintah perlu mempercepat pembentukan Lembaga Pelindungan Data Pribadi yang dibentuk secara independen harus menjalankan perlindungan hukum preventif melalui pengawasan, standarisasi, dan edukasi, serta perlindungan hukum represif melalui pengaduan, pemberian sanksi administratif, dan koordinasi penegakan hukum pidana, guna menjamin perlindungan hak subjek data dan penanggulangan penyalahgunaan teknologi *deepfake* secara efektif dan adil. Selain itu, diperlukan penguatan kapasitas penegak hukum di bidang teknologi forensik digital agar penanggulangan tindak pidana *deepfake* dapat dilakukan secara efektif, berkeadilan, dan adaptif terhadap perkembangan teknologi.

References

Dr. Ismiyanto, S. H. , M. H., Prof. Dr. Edy Lisdiyono, S. H. , M. Hum., & Dr. Krismiyarsi, S. H. , M. Hum. (2025). REFORMULASI KEBIJAKAN HUKUM PIDANA MENGENAI PIDANA KERJA SOSIAL BERBASIS KEADILAN. Penerbit Lawwana.

Firdausi, A., Nur Abadi, F., Yogi Dwi Amelia, T., & Duta Bangsa Surakarta, U. (2025). TINJAUAN ETIS DAN HUKUM TERHADAP PERLINDUNGAN DATA PRIBADI DI TENGAH MARAKNYA KONTEN DEEPFAKE DI MEDIA SOSIAL. Jurnal Hukum Dan Kewarganegaraan, 12(5). https://doi.org/10.3783/causa.v2i9.2461

Iradat, M. A., Ratna, D., & Hariyanto, S. (2025). PT. Media Akademik Publisher. JMA), 3, 3031–5220. https://doi.org/10.62281

Juefei-Xu, F., Wang, R., Huang, Y., Guo, Q., Ma, L., & Liu, Y. (2022). Countering Malicious DeepFakes: Survey, Battleground, and Horizon. International Journal of Computer Vision, 130(7), 1678–1734. https://doi.org/10.1007/s11263-022-01606-8

Koos, S., Shidarta, & Nasution, A. H. (2025). Kecerdasan Artifisial Dalam Hukum Keperdataan. Prenada Media.

Penipuan, D. U., Digital, I., Firdaus, H. S., & Puspita, L. (n.d.). Peran Hukum Dalam Mengatasi Penyebaran Konten. 9, 2025.

Prayoga, H., & Tuasikal, H. (2025). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. Abdurrauf Law and Sharia, 2(1), 22–38. https://doi.org/10.70742/arlash.v2i1.194

Prof. Dr. Barda Nawawi Arief, S. (2008). Bunga Rampai Kebijakan Hukum Pidana : Vol. Cetakan Ke-3 (B. N. Arief, Ed.; Edisi Kedua). Kencana Prenada Media Group.

Prof. Dr. Barda Nawawi Arief, S. (2012). Kebijakan Formulasi Ketentuan Pidana Dalam Peraturan Perundang - Undangan (B. (s) Arief Nawawi, Ed.; Cetakan ke 1). Pustaka Magister.

Rohmati, I., Junaidi, A., & Khaerudi, A. (2024). Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO). 1779–1794.

Sengi, E. SH. M. (2018). Kebijakan Formulasi Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial (M. H. Usak & J. Sabarua Oxianus, Eds.; Cetakan 1). CV. Pilar Nusantara.

Shahzad, H. F., Rustam, F., Flores, E. S., Luís Vidal Mazón, J., de la Torre Diez, I., & Ashraf, I. (2022). A Review of Image Processing Techniques for Deepfakes. In Sensors (Vol. 22, Issue 12). MDPI. https://doi.org/10.3390/s22124556

Syahirah, S. N., Prasetyo, B., Muhammadiyah, U., & Timur, K. (2025). TINJAUAN YURIDIS TERHADAP PENGGUNAAN TEKNOLOGI DEEPFAKE UNTUK PORNOGRAFI MELALUI ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA (Vol. 6, Issue 1). https://ejurnals.com/ojs/index.php/jihk

Wahyudi, E., & Joe, G. (2020). KEBIJAKAN FORMULASI SANKSI PIDANA KEBIRI KIMIA DI INDONESIA YANG AKAN DATANG (Vol. 4, Issue 1). Online. www.voaindonesia.com,

Wahyudi, E., Rifqi, D., & Huda, M. (n.d.). Policy and Law Journal (Polaw) Volume 2 Nomor 1 Tahun 2025 Pelindungan Hukum Atas Data Pribadi Anak dalam Sistem Elektronik: Perspektif UU No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi dan Global.

Zainuddin, M., & Dinda Karina, A. (2023). PENGGUNAAN METODE YURIDIS NORMATIF DALAM MEMBUKTIKAN KEBENARAN PADA PENELITIAN HUKUM USE OF NORMATIVE JURIDICAL METHODS IN PROVING THE TRUTH IN LEGAL RESEARCH. In Smart Law Journal (Vol. 2023, Issue 2). http://stikesyahoedsmg.ac.id/ojs/index.php/sljpISSN2830-6430;eISSN2830-683X