

---

# **URGENSI PENGATURAN PIDANA PENYALAHGUNAAN DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL**

Oleh:

**Michelle Azhari Iradat<sup>1</sup>**

**Diah Ratna Sari Hariyanto<sup>2</sup>**

Universitas Udayana

Alamat: JL. Pulau Bali No.1, Dauh Puri Klod, Kec. Denpasar Bar., Kota Denpasar, Bali, (80114).

Korespondensi Penulis: [michelleazhiradat@gmail.com](mailto:michelleazhiradat@gmail.com), [diah\\_ratna@unud.ac.id](mailto:diah_ratna@unud.ac.id).

**Abstract.** This study aims to analyze the absence of explicit criminal provisions regulating the misuse of deepfake technology in national law and its implications for victim protection. Using a normative juridical research method through statutory and case approaches, this study examines the existing legal framework such as the Electronic Information and Transactions Law (UU ITE), the Sexual Violence Crime Law (UU TPKS), the Personal Data Protection Law, the Criminal Code (KUHP), as well as several deepfake cases in Indonesia including the dissemination of deepfake pornography and digital fraud based on audio-visual manipulation. The findings show that the lack of specific legal norms governing deepfake crimes creates a legal vacuum (rechtsvacuum) and uncertainty in enforcement, making it difficult for law enforcement officers to accurately prosecute perpetrators and leaving victims without adequate guarantees of recovery. This research emphasizes the urgency of establishing a *lex specialis* criminal regulation that not only focuses on punishing offenders but also includes preventive, repressive, and rehabilitative mechanisms for victims through provisions on the right to erase digital traces, restitution, and psychological recovery services with a restorative justice and human rights perspective.

**Keywords:** Deepfake, National Criminal Law, Victim Protection, Legal Vacuum.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE*: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL

**Abstrak.** Penelitian ini memiliki tujuan guna mengkaji ketiadaan pengaturan pidana yang secara eksplisit mengatur penyalahgunaan teknologi *deepfake* dalam hukum nasional serta implikasinya terhadap perlindungan korban. Dengan memanfaatkan teknik penelitian normatif dengan teknik perundang-undangan serta teknik kasus, kajian ini menelaah kerangka hukum yang berlaku seperti UU ITE, UU TPKS, UU Perlindungan Data Pribadi, KUHP, serta beberapa kasus *deepfake* di Indonesia termasuk penyebaran *deepfake* pornografi dan penipuan digital berbasis manipulasi audio-visual. Hasil penelitian menunjukkan bahwa belum adanya norma hukum yang secara spesifik mengatur tindak pidana *deepfake* menyebabkan kosongnya hukum (*rechtsvacuum*) dan ketidakpastian dalam proses penegakan, sehingga aparat penegak hukum kesulitan menjerat pelaku secara tepat dan korban tidak memperoleh jaminan pemulihan yang memadai. Penelitian ini menegaskan urgensi pembentukan regulasi pidana *lex specialis* yang tidak hanya berorientasi pada pemidanaan pelaku, tetapi juga mencakup mekanisme preventif, represif, dan rehabilitatif bagi korban melalui pengaturan hak untuk menghapus jejak digital, restitusi, serta layanan pemulihan psikologis yang berperspektif keadilan restoratif dan HAM.

**Kata Kunci:** *Deepfake*, Hukum Pidana Nasional, Perlindungan Korban, Kekosongan Hukum.

## LATAR BELAKANG

Kemajuan cepat teknologi kecerdasan buatan (*Artificial Intelligence*) telah memicu transformasi yang substansial di beragam dimensi kehidupan manusia modern, termasuk dalam bidang ekonomi, sosial, serta keamanan digital. Salah satu bentuk penerapan kecerdasan buatan yang menimbulkan permasalahan dalam konteks kejahatan siber adalah fenomena *deepfake*, yaitu manipulasi media digital yang dihasilkan dengan teknologi tinggi sehingga memiliki tingkat realisme yang sangat tinggi dan sulit dibedakan dari konten yang asli. Munculnya dan berkembangnya teknologi *deepfake* tidak hanya menghadirkan tantangan teknis, tetapi juga membuka celah penyalahgunaan yang sangat besar dalam aspek perlindungan keamanan sipil, hak privasi individu, serta integritas sistem hukum nasional Indonesia. *deepfake* memanfaatkan kecerdasan buatan guna mengintegrasikan ataupun mengganti wajah individu lainnya ke media audiovisual ataupun foto lainnya, bersamaan dengan kemampuan untuk memanipulasi suara dengan

presisi tinggi sehingga menghasilkan rekaman audio yang secara akustik mirip dengan suara asli target penyalahgunaan.<sup>1</sup> Secara teknis, pembuatan *deepfake* melibatkan proses pelatihan sistem *AI*, menggunakan jaringan neural seperti *generative adversarial networks* (GAN) atau *deep neural networks* (DNN). Dengan memasukkan sejumlah besar data audio, video atau gambar dari seseorang sebagai objek, lalu sistem tersebut menghasilkan versi manipulatif yang menggantikan atau meniru wajah, suara atau gerakan objek asli. Teknik ini dapat mempermudah pelaku menghasilkan konten yang sangat realistik dan sulit dibedakan dari rekaman asli, sehingga menimbulkan tantangan besar di bidang pembuktian dan autentikasi digital.<sup>2</sup>

Penyalahgunaan teknologi *deepfake* menyajikan kerangka risiko yang sangat beragam. Di satu sisi, individu sebagai korban dapat menjadi objek pelanggaran atas hak-kepribadian, seperti hak atas nama baik, privasi, citra diri, dan kontrol atas identitas digitalnya, misalnya ketika wajah atau suara mereka dipakai dalam video pornografi, skema pemerasan, atau penyebaran hoaks.<sup>3</sup> Di sisi lain, dari perspektif publik dan negara, *deepfake* berpotensi merongrong kepercayaan masyarakat terhadap media digital, memfasilitasi penyebaran disinformasi, serta mengancam integritas sistem hukum dan keamanan sipil melalui manipulasi bukti, impersonasi digital, atau sabotase reputasi.<sup>4</sup> Hal ini menegaskan bahwa diperlukan kajian hukum yang lebih mendalam.

Di Indonesia, penyalahgunaan *deepfake* masih belum ditetapkan secara rinci dan tegas dalam ketentuan hukum yang berlaku, walaupun terdapat kasus penyalahgunaan *deepfake* tersebut, salah satunya yaitu kasus seorang mahasiswa Unud berinisial SLKDP tertuduh membuat dan menyebarkan konten porno *deepfake*. Ia mengambil foto mahasiswa dari media sosial, kemudian menggunakan teknologi kecerdasan buatan untuk mengubah foto tersebut menjadi tampak tanpa busana. Sebanyak 35 mahasiswa melapor ke rektorat pada awalnya, namun investigasi internal kemudian mencatat total 37 korban. Kampus menilai perbuatan itu sebagai pelanggaran berat terhadap etika dan kekerasan seksual. Pelaku pun dikenakan sanksi mahasiswa tersebut telah dikeluarkan dari Unud.

---

<sup>1</sup> Prayoga, H. and 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.

<sup>2</sup> Ibid.

<sup>3</sup> Wibowo, K.T. and SH, M., 2025. "Aspek Hukum dalam Dunia Digital. Bandung: Sada Kurnia Pustaka."

<sup>4</sup> Kurniarullah, M.R., Nabila, T., Khalidy, A., Tan, V.J. and Widiyani, H., 2024. "Tinjauan kriminologi terhadap penyalahgunaan artificial intelligence: Deepfake pornografi dan pencurian data pribadi. *Jurnal Ilmiah Wahana Pendidikan*," 10(10), 534-547.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE*: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL

Para korban mengaku trauma seperti merasa takut beraktivitas normal, gelisah, dan resah karena khawatir foto-foto mereka tersebar atau dikenali.<sup>5</sup>

Peraturan hukum yang ada, meliputi Undang Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS), Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi serta KUHP baru (Undang-Undang Nomor 1 Tahun 2023), masih belum merumuskan secara terperinci pengaturan mengenai perbuatan pidana pada konten manipulatif seperti ini.<sup>6</sup>

Permasalahan fundamental lain terletak pada belum maksimalnya jaminan perlindungan hukum pidana bagi korban tindak kriminal *deepfake*. Pada sejumlah kasus, korban mengalami hambatan dalam melaporkan tindak pidana tersebut karena keterbatasan kecakapan instansi penegak hukum mengenai modus operandi *deepfake* dan minimnya alat bukti yang dapat digunakan dalam proses hukum. Disisi lainnya, korban kerap kali menghadapi bentuk viktirisasi ulang, yakni kondisi ketika mereka kembali menjadi sasaran stigma sosial, disalahkan, atau dipermalukan akibat tersebarnya konten palsu di media sosial. Keadaan ini secara nyata melanggar prinsip-prinsip keadilan dan HAM yang selayaknya dijamin dan diberi perlindungan dari negara. Berdasarkan pandangan keadilan restoratif dan perlindungan HAM, negara memiliki tanggungjawab guna merancang tatanan yudisial yang tidak semata-mata terfokus pada pihak pelanggar (*offender-oriented*), namun juga memberi jaminan, pengakuan, serta rehabilitasi yang memadai untuk korban (*victim-oriented*).<sup>7</sup>

Dengan demikian, ketentuan khusus terkait *deepfake* harus dirancang dengan tetap mempertimbangkan hak-hak personal yang terkena dampaknya sebagai bagian dari sistem peradilan pidana yang berkeadilan secara sosial. Absennya regulasi khusus itu sendiri memunculkan kosongnya hukum (*legal vacuum*) dan berdampak pada ketidakjelasan hukum (*legal uncertainty*), terutama untuk aparatur penegak hukum saat memproses pelaku tindak pidana maupun bagi korban dalam mendapatkan keadilan.

<sup>5</sup> kumparanNEWS (2025) “Terungkapnya Kasus Konten Porno Deepfake Mahasiswa Unud”, *kumparan.com*, 27 April”. URL: “<https://kumparan.com/kumparannews/terungkapnya-kasus-konten-porno-deepfake-mahasiswa-unud-24xOaAR2Ntv>” (Diakses 29 November 2025).

<sup>6</sup> Basah, D.A.Y., Wijaya, A. and Januardy, I., 2025. “Kriminalisasi pelanggaran protokol digital: tinjauan hukum pidana terhadap penyebaran deepfake di media sosial.” *Innovative: Journal of Social Science Research*, 5(4), 386-398.

<sup>7</sup> Meliana, Y., 2025. “Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional.” *Jurnal Hukum Lex Generalis*, 6(7). 1-13.

Tindak pidana *deepfake* memberi tuntutan perumusan delik yang mempunyai batasan tegas, aspek tindakan yang terperinci, serta konsep pertanggungjawaban pidana yang mampu menjangkau pelaku dengan pola operandi berbasis digital.<sup>8</sup>

Dengan latar belakang tersebut, penulis dalam pembahasan ini menegaskan urgensi pengaturan hukum pidana yang khusus melindungi korban *deepfake*. Di Indonesia, kebutuhan tersebut semakin mendesak seiring meningkatnya kasus penyalahgunaan media digital. Kerangka hukum pidana Indonesia sebaiknya dikaji ulang agar memasukkan ketentuan yang secara eksplisit mengatur penciptaan dan penyebaran konten *deepfake* tanpa izin, serta mekanisme penegakan hukum yang melindungi kepentingan korban. Dalam penelitian ini penulis mendorong pembaruan regulasi yang responsif terhadap ancaman baru tersebut. Pendekatan pidana diharapkan menjembatani kekosongan hukum yang ada dengan memberikan perlindungan secara eksplisit bagi korban, sekaligus menegaskan akuntabilitas pelaku kejadian *deepfake* dalam sistem hukum Indonesia.

## **METODE PENELITIAN**

Metode penelitian pada jurnal ini adalah studi hukum normatif yang terfokus pada identifikasi dan analisis kekosongan pengaturan pidana terkait penyelewengan dalam penggunaan teknologi *deepfake* dalam hukum nasional. Stud dilakukan melalui sejumlah metode, yakni metode perundang-undangan (statute approach) dan pendekatan kasus. Penelitian ini menggunakan studi kepustakaan sebagai teknik penghimpunan bahan hukum primer, sekunder, dan tersier yang selanjutnya seluruh sumber hukum ditelaah secara kualitatif.

## **HASIL DAN PEMBAHASAN**

### **Urgensi Pengaturan Khusus Dalam Sistem Pidana Nasional Terhadap Problematika Penyalahgunaan Deepfake**

Istilah *deepfake* pertama kali digunakan pada tahun 2017 melalui platform sosial media Reddit.<sup>9</sup> Konsep ini merupakan gabungan dari kata “pembelajaran mendalam”

---

<sup>8</sup> Ibid.

<sup>9</sup> Matthew B. Kugler - Carly Pace. 2021. “*Deepfake* Privacy: Attitudes and Regulation”, SSRN Electronic Journal 116/3, 611-680.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL

(*deep*) dan “palsu” (*fake*). Video *deepfake* dibuat atau diproduksi melalui teknologi GAN (*Generative Adversarial Network*) yang digunakan dalam *Artificial Intelligence (AI)* atau Kecerdasan Buatan. GAN dibentuk dengan menggunakan dua jaringan yang berbeda dengan saat yang bersamaan. Jaringan yang pertama adalah jaringan Generator yang dapat menghasilkan gambar, suara dan data analisis dari *noise* atau *vectors*. Selanjutnya adalah jaringan diskriminasi atau *the discriminator network's* yang akan meningkatkan prediksi realitas gambar agar lebih terlihat realistik.<sup>10</sup> *Deepfake* bisa dipahami sebagai konten media tiruan yang direkayasa secara digital, baik berupa video, gambar, ataupun rekaman audio, yang menampilkan peristiwa atau tindakan yang sebenarnya tidak pernah dilakukan atau terjadi dalam realitas.<sup>11</sup>

Teknologi *deepfake* memanfaatkan kekuatan teknologi pembelajaran mendalam untuk konten audio dan audio visual. Jika diterapkan dengan tepat, model-model ini dapat menghasilkan konten yang secara meyakinkan menunjukkan orang-orang mengatakan atau melaksanakan hal yang tidak mereka perbuat, atau menciptakan orang-orang yang tidak pernah ada sebelumnya.<sup>12</sup> Penggunaan *deepfake* saat ini tidak memiliki batasan tertentu sehingga dapat diakses oleh semua orang. Adanya *tools* dan *software* gratis seperti *deepfacelab* dan *face swap* memudahkan penggunaan *deepfake* tanpa memerlukan *skill* khusus. Ciri pokok *deepfake* yang menjadikannya bermasalah dalam ranah hukum ialah kemampuannya menciptakan materi yang tampak sangat autentik dan mudah dipercaya. Hal ini dapat mengakibatkan risiko pada kredibilitas bukti visual dalam mekanisme penegakan hukum pidana serta berpotensi memicu keresahan sosial, misalnya melalui persebaran informasi palsu atau tuduhan tanpa dasar secara luas. Dalam studi pada September 2019, *Sensity* menemukan bahwa 96% video palsu melibatkan pornografi non-konsensual. Untuk membuat video ini, wajah korban akan di-*overlay* pada tubuh pelaku pornografi sehingga tampak seolah-olah korban yang sedang melakukan aksi pornografi tersebut dan terdapat beberapa situs pornografi yang secara khusus

---

<sup>10</sup> Rana, M.S., Nobi, M.N., Murali, B. and Sung, A.H., 2022. “Deepfake detection: A systematic literature review.” *IEEE access*, 10, 25494-25513.

<sup>11</sup> Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A. and Dwivedi, Y.K., 2023. “Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, 113368.”

<sup>12</sup> Europol. (2022). “Facing reality? Law enforcement and the challenge of deepfakes: An Observatory report from the Europol Innovation Lab. Publications Office of the European Union, 7.”

memproduksi *deepfake* pornografi. Pelaku seringkali bertindak secara anonim, sehingga mempersulit identifikasi kejahatan.<sup>13</sup>

Di Indonesia, kasus penyalahgunaan *deepfake* sudah banyak terjadi. Dilansir dari Media Indonesia: “Bahaya Penggunaan *Deepfake*: Ini Kasus *Deepfake* di Indonesia” kasus *deepfake* di indonesia mengalami lonjakan sebesar 1550% antara tahun 2022 dan 2023. Salah satunya adalah kasus *deepfake* Pada awal tahun 2025, Direktorat Tindak Pidana Siber (Bareskrim Polri) menjelaskan sebuah sindikat penipuan memanfaatkan teknologi kecerdasan buatan (AI) khususnya modus *deepfake* yang memanipulasi video dan audio dari pejabat tinggi negara. Dilansir dari CNN: “Modus Penipuan *Deepfake* AI Prabowo-Gibran Tawarkan Bantuan Barang” *deepfake* yang memanipulasi video dan audio dari pejabat tinggi negara. Pelaku utama (inisial AMA, usia 29 tahun, berasal dari Lampung Tengah) ditangkap pada 16 Januari 2025. Dalam aksinya, tersangka menggunakan rekaman video pejabat yang diubah narasinya sehingga seolah-olah menyampaikan bantuan kepada masyarakat, kemudian menyebarluaskan konten tersebut melalui platform media sosial untuk mengelabui korban agar melakukan pembayaran atau mentransfer sejumlah uang. Menurut kepolisian, terdapat setidaknya 11 korban dalam kurun waktu sekitar empat bulan, dengan total kerugian mencapai ± Rp 30 juta. Pelaku juga diduga bekerja dalam jaringan dengan tersangka lain (inisial FA) yang saat ini berstatus DPO (daftar pencarian orang). Sebagai konsekuensi dari tindakannya, AMA dikenai pasal 51 ayat (1) jo pasal 35 UU No. 1 Tahun 2024 tentang ITE dan pasal 378 KUHP.<sup>14</sup>

Kemudian kasus lainnya adalah seorang mahasiswa Universitas Udayana (UNUD) Bali, berinisial S, disinyalir memproduksi materi pornografi rekayasa dengan memanfaatkan kecerdasan artifisial melalui teknologi *deepfake*. Dilansir dari Kompas: “Mahasiswa Universitas Udayana Bali Diduga Bikin Konten Porno Palsu Berbasis AI.” Modus operandi yang dilaporkan antara lain: pelaku diduga mengambil secara tidak sah foto-mahasiswa (teman sekampus atau sesama fakultas) melalui media sosial (Instagram),

---

<sup>13</sup> Castro, D. (2020) “Deepfakes Are on the Rise — How Should Government Respond?,” *GovTech*. URL: <https://www.govtech.com/policy/deepfakes-are-on-the-rise-how-should-government-respond.html> (Diakses 29 November 2025).

<sup>14</sup> CNN Indonesia (2025) “Modus penipuan *deepfake* AI, Prabowo-Gibran tawarkan bantuan uang,” *CNN Indonesia*, 24 Januari. URL: <https://www.cnnindonesia.com/nasional/20250124072755-12-1190915/modus-penipuan-deepfake-ai-prabowo-gibran-tawarkan-bantuan-uang> (Diakses 29 November 2025)

## **URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE*: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL**

kemudian mengubah foto tersebut menjadi gambar “telanjang” atau konten vulgar menggunakan bot berbasis kecerdasan buatan (*AI*) via aplikasi Telegram. Hingga saat ini, sejumlah media mencatat bahwa sebanyak 35 hingga 37 korban (mahasiswa) telah melapor ke pihak rektorat atau Dewan Etik Fakultas UNUD. Namun korban hingga saat ini enggan melapor ke pihak berwajib.<sup>15</sup>

Kedua kasus tersebut memperlihatkan bahwa penyalahgunaan *deepfake* mencerminkan degradasi nilai moral dan penggunaan teknologi. Penyalahgunaan *deepfake* dapat merugikan individu maupun kelompok dalam skala besar, yang dapat berdampak pada psikologis yang mendalam bagi korban seperti trauma, rasa malu, dan kehilangan rasa aman di lingkungan sosial, kemudian penyalahgunaan *deepfake* dapat mengancam integritas informasi publik. Melalui kasus yang telah dijabarkan diatas, manipulasi video pejabat negara dapat berpotensi menimbulkan disinformasi dan intabilitas sosial, yang dapat menurunkan tingkat kepercayaan masyarakat terhadap lembaga pemerintahan yang pada akhirnya akan menggerus legitimasi otoritas negara.

Persoalan penyalahgunaan *deepfake* semakin kompleks apabila tidak ditangani dengan serius karena *deepfake* mampu berevolusi dengan amat cepat dalam rentang waktu yang relatif pendek. Konten *deepfake* kerap kali tampak begitu autentik serta menyebar secara masif di beragam jejaring sosial digital. Keaslian video atau suara memerlukan keahlian digital forensik. Sebaliknya, jejaring sosial belum mempunyai tata kelola internal yang cukup untuk mendeteksi ataupun memberi penanda pada konten *deepfake*. Beragam studi sudah menggarisbawahi ancaman yang ditimbulkan oleh teknologi *deepfake* atas privasi, kebebasan berekspresi, serta integritas penegakan hukum. Dengan mempertimbangkan kompleksitas dampak yang ditimbulkan oleh perkembangan teknologi *deepfake*, diperlukan suatu metode hukum yang memiliki karakter yang terus berkembang dan mampu menyesuaikan diri dengan perubahan pesat dalam perkembangan teknologi informasi.

Hukum nasional memiliki beberapa aturan yang mengatur secara menyeluruh tentang penjagaan hak kerahasiaan, informasi personal, serta pembatasan-pembatasan atas praktik pemanfaatan perangkat elektronik untuk berbuat tindak kriminal. Pada dasarnya, aturan ini bisa menjadi acuan untuk pencegahan, atau memberikan sanksi

---

<sup>15</sup> kumparanNEWS, Loc.Cit

terhadap penyalahgunaan *deepfake* di Indonesia. Konstitusi Indonesia telah menetapkan jaminan yuridis bagi setiap individu guna mewujudkan rasa tenteram serta memastikan pemenuhan hak-hak fundamental manusia.<sup>16</sup> Dalam pasal 28G ayat (1) Undang-Undang Dasar 1945 menjelaskan bahwasanya: “*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*” Selanjutnya, dalam Pasal 28H ayat (4) Undang-Undang Dasar 1945 yang mengatur mengenai Hak Privasi yang mengemukakan bahwasanya: “*Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun.*”.

Dengan ditetapkannya jaminan atas keselamatan diri serta kepemilikan pribadi individu dalam Undang-Undang Dasar 1945, sebagai hasilnya tiap penduduk mempunyai hak yang dijamin konstitusi, sementara negara berkewajiban memberi perlindungan menyeluruh pada rakyat serta memenuhi tuntutan konstitusional itu sendiri.<sup>17</sup>

Salah satu turunan dari pasal 28G ayat (1) Undang-Undang Dasar 1945 adalah Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.<sup>18</sup> *Deepfake* adalah bentuk media rekayasa yang memanfaatkan identitas pihak lain dan berpotensi merusak reputasi serta martabat individu. Praktik demikian pada prinsipnya dapat dikualifikasikan pada Pasal 27A, yang memuat ketentuan mengenai tindakan yang menjatuhkan martabat maupun reputasi seseorang termasuk perbuatan penistaan dan/atau pencemaran melalui fitnah yang menimbulkan kerugian bagi korban. Aturan lainnya yang dapat dijadikan acuan dalam praktik penyalahgunaan *deepfake* adalah Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi pada pasal 65 ayat (3), Pasal 66, Pasal 67, ayat (3) dan Pasal 68. UU RI No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan melalui Pasal 65 ayat (3) larangan tiap individu untuk secara melawan hukum menggunakan data

<sup>16</sup> Latifatunnisa, R., & Yudha, M. W. (2025). “Urgensi pembaruan regulasi dalam menanggulangi penyalahgunaan teknologi artificial intelligence dan *deepfake* di Indonesia: Perspektif perlindungan hak privasi.” *CAUSA*, 1(2), 235–265.

<sup>17</sup> Kusnadi, S. A., & Wijaya, A. U. (2021). “Perlindungan hukum data pribadi sebagai hak privasi.” *Al-Wasath*, 2(1), 20.

<sup>18</sup> Noerman, C. T., & Ibrahim, A. L. (2024). “*Kriminalisasi deepfake di Indonesia sebagai bentuk perlindungan negara.*” *USM Law Review*, 7(2), 610.

## **URGENSI PENGATURAN PIDANA PENYALAHGUNAAN DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL**

pribadi yang bukan miliknya, kemudian melalui Pasal 66 kriminalisasi pembuatan atau pemalsuan informasi pribadi untuk memperoleh keuntungan pribadi atau individu lainnya yang berpotensi merugikan pihak lain, serta diperkuat dengan Pasal 67 ayat (3) yang menjatuhkan sanksi pidana kurungan selama tidak lebih dari 5 tahun dan sanksi uang maksimal Rp5.000.000.000,00 (lima miliar rupiah) bagi penggunaan tidak sah data pribadi dan Pasal 68 yang mengancam pidana lebih berat, kurungan selama tidak lebih dari 6 tahun dan sanksi uang maksimal Rp6.000.000.00,00 (enam miliar rupiah) bagi pemalsuan/fabrikasi data, sehingga keseluruhan norma tersebut membentuk rezim perlindungan yang berorientasi pada kontrol subjek data, integritas identitas, dan efek jera yang proporsional. Kemudian, pada konteks hukum pidana di Indonesia, pendekatan yang diterapkan melalui ketentuan-ketentuan dalam KUHP terkait perusakan reputasi (Pasal 310-311 KUHP).<sup>19</sup>

Namun, Pasal-Pasal dari Undang-Undang yang berlaku tersebut masih dianggap memiliki cakupan yang terlalu luas sehingga belum mencakup unsur-unsur teknologi yang secara khusus berkaitan dengan *deepfake*. Adanya tindakan pidana terhadap penyelewengan *deepfake* selayaknya mampu ditanggulangi melalui aplikasi regulasi yang tegas. Tetapi, ketiadaan ketentuan di Indonesia yang secara spesifik mengatur tentang *deepfake* secara eksplisit dapat menyebabkan kekosongan hukum yang menimbulkan ketidakpastian hukum. Kondisi ini disebabkan oleh ketidakpastian terkait langkah yang perlu ditempuh guna mengantisipasi serta menangani perbuatan melawan hukum berupa *deepfake*.<sup>20</sup> Di Indonesia, Diperlukan suatu kerangka hukum pidana yang komprehensif untuk mengatur penggunaan teknologi *deepfake* dan berorientasi preventif, tidak hanya berfokus pada aspek penindakan terhadap pelaku penyebaran *deepfake*, tetapi juga mencakup mekanisme pencegahan, peningkatan literasi digital masyarakat, serta upaya pemulihan dan perlindungan bagi korban penyalahgunaan teknologi tersebut. Sudarto menjabarkan bahwasanya hukum pidana bukan semata-mata berfungsi menjadi sarana penanganan tindak kriminal, melainkan juga berkewajiban memberikan penjaminan serta perlindungan yuridis bagi publik.<sup>21</sup>

---

<sup>19</sup> Latifatunnisa & Yudha, *Op.Cit.*, 6.

<sup>20</sup> Noerman & Ibrahim, *Op.Cit.*, 612.

<sup>21</sup> Sudarto (1986) *Hukum dan Hukum Pidana*. Bandung: Alumni. 15.

Tindak pidana penyalahgunaan *deepfake* yang belum diatur secara eksplisit pada Kitab Undang-Undang Hukum Pidana ataupun pada Undang-Undang Informasi dan Transaksi Elektronik, berdampak pada aparatur penegak hukum yang berpotensi menghadapi kendala saat menentukan sanksi pidana yang relevan terhadap pelaku serta memperbesar potensi terjadinya pelanggaran terhadap individu maupun masyarakat. Pada studinya, Lestari dan Alamsyah (2022) mengemukakan bahwasanya tidak adanya aturan spesifik terkait *deepfake* menimbulkan ruang hampa normatif yang menyebabkan pihak terdampak mengalami hambatan dalam memperoleh keadilan.<sup>22</sup>

Adanya teknologi *deepfake* banyak disalahgunakan dalam beragam macam tindak kriminal, mulai dari perusakan reputasi, pemerasan, pornografi tanpa persetujuan, praktik penipuan, hingga rekayasa politik.<sup>23</sup> Dengan demikian, tiap variasi tindak kriminal baru yang mempunyai ciri khas tertentu dan berpotensi mengancam urgensi yuridis wajib memperoleh tanggapan normatif yang proporsional melalui perumusan sanksi pidana yang lebih terarah. Pengaturan yang eksplisit terhadap penyalahgunaan *deepfake* merupakan langkah yang strategis dalam berkontribusi terhadap pembentukan sistem hukum pidana yang mampu menyesuaikan diri dengan kemajuan teknologi serta tanggap terhadap perubahan sosial dan digital. Sebagaimana yang diungkapkan oleh Barda Nawawi Arief, bahwasanya modernisasi hukum pidana Indonesia perlu ditujukan pada perumusan kaidah hukum yang sanggup merespons berbagai tantangan kriminalitas kontemporer, mencakup tindak kejahatan yang bertumpu pada teknologi.<sup>24</sup>

Negara-negara lain telah menunjukkan 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, misalnya, Korea Selatan memilih jalur pemidanaan langsung atas *deepfake* seksual non-konsensual. Revisi peraturan perundang-undangan kejahatan seksual tahun 2024-2025 menegaskan bahwa pembuatan, distribusi, bahkan kepemilikan atau menonton *deepfake* seksual tanpa persetujuan merupakan perbuatan pidana, dengan ancaman pidana kurungan dan/atau denda yang signifikan. Kebijakan ini berangkat dari lonjakan kasus dan dampak korban (terutama perempuan dan remaja), serta kebutuhan perangkat

---

<sup>22</sup> Kurniarullah, Nabilah, Khalidy, Tan & Widiyani, *loc. cit.*

<sup>23</sup> Schick, N. (2020). *Deepfakes: The coming infocalypse*. London: Hachette UK, 78-82.

<sup>24</sup> Arief, B. N. (2016). “Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru (Edisi ke-2).” Jakarta: Kencana Prenada Media, 121

## **URGENSI PENGATURAN PIDANA PENYALAHGUNAAN DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL**

penegakan untuk penghapusan cepat konten ilegal dan layanan dukungan korban. Dengan demikian, Korea Selatan menempatkan perlindungan martabat dan keselamatan seksual sebagai kepentingan hukum utama, melampaui sekadar kewajiban pelabelan.<sup>25</sup> Selain Korea Selatan, Tiongkok juga mengatur *deepfake* secara spesifik melalui “*Administrative Provisions on Deep Synthesis in Internet-Based Information Services (2023)*.” Aturan ini mewajibkan penyedia layanan “sintesis mendalam” (*deep synthesis*) untuk menandai konten sintetis, memastikan keamanan algoritma, serta memenuhi kewajiban *filing* dan tata kelola risiko. Larangan berfokus pada penyediaan layanan yang menyesatkan, mengancam ketertiban publik, atau melanggar hak subjek data/identitas; sedangkan kewajiban berfokus pada *traceability* (termasuk *watermarking*) dan *due diligence* atas konten. Secara kebijakan, pendekatan ini menggabungkan kewajiban teknis (penandaan/*watermark*) dan pengawasan administratif, sehingga memadukan pencegahan, *compliance*, dan sanksi administratif-pidana bila terjadi pelanggaran serius.<sup>26</sup> Serta masih terdapat beragam negara lainnya yang sudah menetapkan regulasi khusus terkait penyalahgunaan *deepfake*.

Melalui regulasi-regulasi yang secara khusus diatur mengenai penyalahgunaan *deepfake* oleh beberapa negara, dapat disimpulkan bahwa di Indonesia, terkhususnya hukum pidana, memerlukan regulasi yang secara eksplisit mengatur mengenai penyalahgunaan *deepfake* sebab menjadi keperluan yang mendesak untuk memastikan jaminan yuridis serta pemerataan keadilan. Dalam ranah hukum pidana nasional, pola delik formil yang diterapkan dalam KUHP menjadikan beragam perkara distribusi konten *deepfake* sukar dikategorikan sebagai perbuatan pidana. Terlebih lagi apabila pembuat atau penyebar konten tersebut mengunggahnya melalui platform yang servernya berlokasi di luar wilayah kewenangan yuridis Indonesia.<sup>27</sup> Sehingga dengan adanya regulasi yang eksplisit mengenai penyalahgunaan *deepfake* di Indonesia akan memberikan dampak yang signifikan, karena dapat memberikan perlindungan yang lebih tegas terhadap individu dari potensi kerugian reputasional dan pelanggaran privasi. Dengan adanya aturan yang jelas, negara akan mampu menanggulangi penyebaran konten

---

<sup>25</sup> Reuters. (2024). “South Korea criminalises watching or possessing sexually explicit deepfakes.” Reuters. 34.

<sup>26</sup> Zhang, L. (2023) “China: Provisions on Deep Synthesis Technology Enter into Effect,” *Global Legal Monitor / Library of Congress*, 25 April. URL: <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/> (Diakses 29 November 2025).

<sup>27</sup> Noerman & Ibrahim, *Loc.Cit.*, 612.

manipulatif yang dapat merusak tatanan sosial, meminimalkan disinformasi, serta memberikan kepastian hukum bagi korban dan pelaku, sekaligus memperkuat integritas sistem informasi di ruang digital. Regulasi semacam ini juga akan membuka peluang untuk penegakan hukum yang lebih efektif, menciptakan ruang bagi teknologi yang lebih bertanggung jawab, dan mendukung terciptanya lingkungan digital yang lebih aman dan transparan. Oleh karena itu, penyusunan delik pidana khusus terkait *deepfake* menjadi kebutuhan mendesak agar hukum nasional mampu beradaptasi dengan perkembangan teknologi, menjamin keamanan digital, serta memastikan hak-hak korban memperoleh perlindungan yang layak dan proporsional dalam sistem peradilan pidana Indonesia.

### **Perlindungan Hukum Pidana Terhadap Korban Kejahatan *Deepfake* Ditinjau Melalui Aspek Keadilan Restoratif dan Hak Asasi Manusia**

Dalam era digitalisasi modern, kemunculan teknologi *deepfake* telah melahirkan bentuk kejahatan baru yang mengancam hak-hak mendasar para korban. Manipulasi konten visual dan audio berbasis kecerdasan buatan ini berpotensi menimbulkan resiko yang merugikan hak konstitusional warga negara jika digunakan dengan tujuan seperti menyebarluaskan berita yang tidak benar, merusak nama baik, memanipulasi opini publik atau mengganggu hak privasi seseorang. Selain itu, penyalahgunaan *deepfake* juga akan mengganggu tatanan sosial dan nilai-nilai moral yang menjunjung tinggi integritas seseorang. Sehingga memunculkan kebutuhan mendesak akan jaminan perlindungan hukum pidana yang memadai bagi para korban. Pasal 28D ayat (1) UUD 1945 menyatakan bahwa “setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum, yang dapat merugikan harkat dan martabat manusia.” Kemudian pasal 28J ayat (2) juga menetapkan bahwa kemerdekaan berekspresi harus tunduk pada hukum demi menghormati hak orang lain dan menjaga moralitas, keamanan serta ketertiban. Selain itu Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia, pada Pasal 29 ayat (1) menyatakan bahwasanya “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya” dan pasal 30 yang mengemukakan bahwasanya “Setiap orang berhak atas rasa aman dan tenteram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu”.

## **URGENSI PENGATURAN PIDANA PENYALAHGUNAAN DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL**

Dalam ranah hukum pidana nasional, penyintas tindak kejahatan *deepfake* masih belum mendapatkan sorotan maupun jaminan perlindungan yang layak. Mayoritas ketentuan perundang-undangan tetap terkonsentrasi pada pelaku, sementara aturan mengenai perlindungan terhadap pihak yang dirugikan belum tertuang secara tegas dan sistematis. Padahal, dari sudut pandang keadilan, korban adalah orang yang paling merasakan dampak serta berhak menerima perlakuan dan pemulihan yang sebanding.<sup>28</sup> Menurut Komnas Perempuan, insiden kekerasan berbasis gender di ruang daring (KGBO) pada area publik, Komnas Perempuan merekam sebanyak 876 perkara kekerasan berdasar gender yang dilaporkan pada tahun 2022 dan pada tahun terjadi peningkatan menjadi 1.801 kasus. Kasus tersebut tergolong tindakan pendistribusian gambar ataupun rekaman bermuatan pornografi yang dibuat melalui teknologi *deepfake*.<sup>29</sup> Merujuk pada perspektif HAM, negara berkewajiban melindungi penduduknya dari pelanggaran yang dilakukan oleh individu maupun kelompok lain. Prinsip *due diligence* menurut hukum internasional menuntut negara guna mengambil langkah pencegahan, melakukan penyelidikan, menjatuhkan sanksi atas pelanggaran HAM, dan menyediakan mekanisme pemulihan yang efektif bagi korban.<sup>30</sup> Sehingga, apabila negara tidak berupaya dalam mencegah dan mengurangi penyalahgunaan *deepfake*, maka negara dapat dianggap gagal dalam melindungi masyarakatnya, karena tidak adanya regulasi khusus yang mengatur mengenai penyalahgunaan *deepfake* baik untuk pelaku maupun korban itu sendiri.

Ketiadaaan regulasi dan atau pembentukan ketentuan yuridis yang bersifat spesifik mengenai pemanfaatan *deepfake* menimbulkan kekosongan norma dalam sistem hukum, atau istilahnya *rechtsvakuum*. Dengan kata lain, masih belum ada ketentuan yang secara jelas dan tegas menetapkan terkait penggunaan teknologi *deepfake* sebagai bentuk tindak pidana yang menyebabkan munculnya kekosongan hukum. Kekosongan ini memberikan ruang bagi pelaku yang menggunakan *deepfake* untuk tujuan negatif. Situasi ini menimbulkan ketidakpastian hukum (*legal uncertainty*), sehingga para korban mengalami kesulitan memperoleh keadilan lantaran aparatur hukum juga tidak

---

<sup>28</sup> Latifatunnisa & Yudha, *Op. Cit.* 9.

<sup>29</sup> Komnas Perempuan. (2023). “Kekerasan terhadap perempuan di ranah publik dan negara: Minimnya perlindungan dan pemulihan, kekerasan siber berbasis gender (CATAHU 2023: Catatan Tahunan Kekerasan terhadap Perempuan Tahun 2022).” Jakarta: Komnas Perempuan, 100.

<sup>30</sup> Muladi. (2002). “Hak asasi manusia, politik, dan sistem peradilan pidana.” Jakarta: Badan Pembinaan Hukum Nasional, 72.

mempunyai pedoman yang jelas untuk melakukan tindakan.<sup>31</sup> Gangguan stres pascatrauma (PTSD) adalah salah satu dampak psikologis yang dapat dialami oleh korban *deepfake*. Menurut Miao dkk. (2018), PTSD merupakan kelainan psikologis yang lazim muncul setelah individu menghadapi kejadian yang bersifat traumatis. Kondisi ini memiliki gambaran klinis yang beragam, namun ditandai oleh gejala yang mengacaukan fungsi kognitif, suasana emosional, menimbulkan respons fisik tertentu, serta mengubah pola perilaku. PTSD mampu menimbulkan disfungsi jangka panjang, memicu gangguan mental penyerta, dan menambah kerentanan terhadap tindakan bunuh diri. Setiap kali seorang korban dihadapkan pada penghinaan terhadap martabatnya, terutama yang berlandaskan fitnah, keinginan untuk memulihkan reputasi baik mereka tentu menjadi hal terpenting yang ingin dilakukan korban.<sup>32</sup> Dalam kasus *deepfake*, hak untuk menghapus, juga dikenal sebagai RtBF (*Right to Be Forgotten*), idealnya menjadi salah satu hak yang dapat diakses dengan mudah oleh korban. Apabila penegakan hukum terlalu berfokus pada penindakan terhadap pelaku, maka diperlukan jaminan yang seimbang bahwa pemenuhan dan perlindungan hak-hak fundamental korban tetap terpenuhi secara memadai.

Hak atas privasi dan kehormatan individu ialah komponen fundamental dari HAM yang wajib dilindungi secara absolut. Pasal 28G ayat (1) UUD 1945 secara tegas menyediakan jaminan yuridis yang menyeluruh bagi setiap penduduk, meliputi penjagaan atas keseluruhan diri, kesatuan keluarga, harga diri pribadi, harkat kemanusiaan, serta hak atas kepemilikan aset, sekaligus memastikan hak mendasar guna menikmati rasa aman dari berbagai kemungkinan bahaya, baik yang bersifat jasmani ataupun nonjasmani. Sehingga negara berkewajiban dalam menjamin hak-hak tersebut. Ketidakmampuan negara dalam pencegahan serta bertindak atas tindakan kriminal *deepfake* membuat Pasal tersebut terkesan menjadi paradoksial karena konten *deepfake* yang menghancurkan moral individu secara langsung merupakan pelanggaran terhadap nilai tersebut. Dengan demikian, tatanan hukum pidana perlu menyediakan kepastian penjagaan atas hak-hak

---

<sup>31</sup> Hasbi & Rokhanah. (2019). “*Hukum materiil syariah*.” Banten: La Tansa Mashiro Publisher, 70.

<sup>32</sup> Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2024). “From trauma to recovery: How victim-centered approaches can combat *deepfake* pornography.” *Pakistan Journal of Life and Social Sciences*, 22(2), 15211.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE*: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL

tersebut secara optimal. Di samping pendekatan yuridis, penjaminan pada korban turut memerlukan metode bersifat psikososial.<sup>33</sup>

Dalam Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP) yang berbunyi: “*Tiada suatu perbuatan dapat dipidana, kecuali berdasarkan kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelumnya.*” Prinsip ini memastikan bahwasanya individu hanya bisa dikenai sanksi pidana apabila tindakannya secara tegas telah ditetapkan dalam ketentuan hukum pidana. Mengingat pemanfaatan *deepfake* belum mempunyai rumusan serta aturan yang jelas dalam sistem hukum Indonesia, sebagai hasilnya aparatur hukum kesulitan guna mengidentifikasi dan menempatkan perbuatan tersebut secara akurat dalam ranah pemidanaan.<sup>34</sup> Korban kerap mengalami hambatan dalam menunjukkan autentisitas serta motif buruk yang melatarbelakangi peredaran konten informasi palsu itu sendiri. Kondisi ini menegaskan pentingnya keberadaan instrumen yuridis yang tidak semata-mata bersifat penindakan, tetapi juga pencegahan, seperti prosedur *takedown* konten digital dan keterlibatan pakar forensik digital.

Penyalahgunaan *deepfake* merugikan korban baik secara materiil maupun imateriil. Definisi korban kejahatan dapat ditemukan dalam hasil United Konferensi Negara-negara yang diadakan di Milan, Italia pada bulan September 1985, yang menegaskan bahwa Korban merupakan individu atau sekelompok orang yang telah mengalami dampak merugikan, mencakup rasa sakit fisik maupun psikis, tekanan emosional, kerugian finansial, atau terampasnya hak-hak mendasar mereka, baik akibat perbuatan maupun kelalaian pihak lain.<sup>35</sup> Kemudian, menurut Pasal 1 angka 3 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, “Korban adalah orang yang mengalami kekerasan fisik, kerugian mental dan/atau ekonomi yang disebabkan oleh suatu kejahatan”. Sehingga dalam hal ini, korban penyalahgunaan *deepfake* harus menjadi fokus negara untuk melindungi rakyatnya. Mahkamah Konstitusi Republik Indonesia melalui Putusan MK Nomor 166/PUU-XXI/2023 menegaskan bahwasanya norma Pasal 1 angka 35 Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum, khususnya

<sup>33</sup> Komnas Perempuan. (2021). “*Laporan tahunan kekerasan berbasis gender siber.*” Jakarta: Komnas Perempuan.

<sup>34</sup> Kusnadi, S. A., & Putri, D. W. S. (2025). “Perlindungan hak privasi dalam penyalahgunaan teknologi *deepfake* di Indonesia.” *Jurnal RechtsVinding*, 14(2), 195–210.

<sup>35</sup> Noviantama, D., & Rahman, A. A. (2024). “*Deepfake: A review from the victimology perspective.*” ISSN 3064-3019.

frasa “*citra diri*” terkait foto atau gambar peserta pemilu, harus ditafsirkan secara bersyarat dengan ketentuan bahwa peserta pemilu wajib menyajikan foto atau gambar pribadi yang asli, terkini, serta tidak mengalami rekayasa ataupun manipulasi berlebihan menggunakan teknologi *artificial intelligence* (AI).<sup>36</sup> Putusan Mahkamah Konstitusi tersebut adalah suatu inovasi regulasi yang menghadirkan arah dan pedoman etis bagi penyalahgunaan kecerdasan buatan di Indonesia, salah satunya adalah *deepfake*. Melalui putusan tersebut, isu terkait penggunaan *deepfake* dapat dipandang sebagai persoalan konstitusional yang memerlukan perhatian khusus dari pemerintah untuk ditetapkan secara rinci melalui regulasi hukum yang berlaku.

Pada kondisi ini, perlindungan korban idealnya meliputi tiga lapis urgensi. Pertama, perlindungan preventif, berupa aturan yang secara jelas melarang pembuatan dan penyebaran konten *deepfake* tanpa persetujuan, disertai mekanisme deteksi dan penghapusan otomatis sebagai bentuk mitigasi kerusakan reputasi. Kedua, perlindungan represif, yaitu pidana tegas bagi pelaku yang tidak hanya mencakup pennenjaraan atau denda, tetapi juga restitusi dan tanggung jawab untuk menghilangkan jejak digital yang merugikan korban. Ketiga, perlindungan rehabilitatif, yang berorientasi pada pemulihan korban melalui konseling psikologis, bantuan hukum, dan akses terhadap *Right to Be Forgotten* sebagai bentuk pemulihan martabat.

## KESIMPULAN DAN SARAN

Urgensi pengaturan pidana terkait penyalahgunaan *deepfake* terletak pada ketiadaan norma khusus yang mengatur secara tegas bentuk perbuatan, unsur tindak pidana, serta sanksi bagi pelaku, sehingga menciptakan *rechtsvacuum* dan ketidakpastian hukum dalam proses penegakan. Tanpa regulasi yang jelas, aparat kesulitan membuktikan intensi pelaku serta menetapkan delik, sementara korban tidak memperoleh jaminan perlindungan dan pemulihan yang memadai. Kondisi ini diperparah dengan dampak serius yang ditimbulkan, baik berupa kerugian psikologis, reputasional, maupun pelanggaran privasi yang sering kali sulit dipulihkan. Oleh karena itu, pembentukan norma hukum pidana *lex specialis* menjadi mendesak sebagai dasar pemidanaan yang spesifik sekaligus memberikan kepastian hukum dalam penindakan.

---

<sup>36</sup> Kusnadi & Putri, *Op.Cit.*, 205.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE*: TELAAH ASPEK PERLINDUNGAN KORBAN DALAM HUKUM NASIONAL

Dari aspek perlindungan korban, sistem hukum saat ini belum menyediakan mekanisme pemulihan yang komprehensif dan berorientasi pada korban. Perlindungan ideal harus mencakup: (1) perlindungan preventif melalui larangan eksplisit, deteksi automatis, dan hak penghapusan konten (*right to be forgotten*); (2) perlindungan represif dengan sanksi pidana, restitusi, dan kewajiban penghapusan jejak digital oleh pelaku; serta (3) perlindungan rehabilitatif berupa layanan psikologis, bantuan hukum, dan pemulihan martabat korban. Dengan demikian, urgensi perlindungan korban bukan hanya terkait penghukuman pelaku, tetapi pada terciptanya sistem hukum yang mampu menjamin pemulihan hak, keamanan digital, dan perlindungan penuh terhadap identitas pribadi korban sesuai prinsip keadilan restoratif dan HAM.

## DAFTAR REFERENSI

### Buku

Arief, B. N. (2016). *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru* (Edisi ke-2). Jakarta: Kencana Prenada Media.

Sudarto (1986) *Hukum dan Hukum Pidana*. Bandung: Alumni.

Wibowo, K.T. and SH, M., 2025. *Aspek Hukum dalam Dunia Digital*. Bandung: Sada Kurnia Pustaka.

### Artikel Jurnal

Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025). Kriminalisasi pelanggaran protokol digital: Tinjauan hukum pidana terhadap penyebaran *deepfake* di media sosial. *Innovative: Journal of Social Science Research*, 5(4), 386–398.

Europol. (2022). *Facing reality? Law enforcement and the challenge of deepfakes: An Observatory report from the Europol Innovation Lab*. Publications Office of the European Union.

Hasbi, & Rokhanah. (2019). *Hukum materiil syariah*. La Tansa Mashiro Publisher.

Hutchinson, T. (2015). The doctrinal method: Incorporating interdisciplinary methods in reforming the law. *Erasmus Law Review*, 8(3), 132.

Komnas Perempuan. (2021). *Laporan tahunan kekerasan berbasis gender siber*. Komnas Perempuan.

Komnas Perempuan. (2023). *CATAHU 2023: Kekerasan terhadap perempuan di ranah publik dan negara, kekerasan siber berbasis gender*. Komnas Perempuan.

Kugler, M. B., & Pace, C. (2021). *Deepfake* privacy: Attitudes and regulation. *SSRN Electronic Journal*, 116(3), 611–680.

Kusnadi, S. A., & Putri, D. W. S. (2025). Perlindungan hak privasi dalam penyalahgunaan teknologi *deepfake* di Indonesia. *Jurnal RechtsVinding*, 14(2), 195–210.

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al-Wasath*, 2(1), 20.

Latifatunnisa, R., & Yudha, M. W. (2025). Urgensi pembaruan regulasi dalam menanggulangi penyalahgunaan teknologi artificial intelligence dan *deepfake* di Indonesia: Perspektif perlindungan hak privasi. *CAUSA*, 1(2), 235–265.

Mekhail, M., Mustak, M., et al. (2022). *Deepfakes*: Deceptions, mitigations, and opportunities. *Journal of Business Research*, 154, 1.

Muladi. (2002). *Hak asasi manusia, politik, dan sistem peradilan pidana*. Badan Pembinaan Hukum Nasional.

Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2024). From trauma to recovery: How victim-centered approaches can combat *deepfake* pornography. *Pakistan Journal of Life and Social Sciences*, 22(2), 15211.

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi *deepfake* di Indonesia sebagai bentuk pelindungan negara. *USM Law Review*, 7(2), 610–612.

Noviantama, D., & Rahman, A. A. (2024). *Deepfake*: A review from the victimology perspective. *ISSN 3064-3019*.

Prayoga, H. and 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.

Rana, M. S., et al. (2022). *Deepfake* detection: A systematic literature review. *IEEE Access*, 10, 25494–25513.

Schick, N. (2020). *Deepfakes: The coming infocalypse*. Hachette UK.

Susanti Kusumastuti, D. O. (2021). Urgensi pengaturan khusus tindak pidana siber dalam sistem hukum pidana Indonesia. *Jurnal Yudisia*, 14(1), 45–60.

# URGENSI PENGATURAN PIDANA PENYALAHGUNAAN *DEEPCODE: TELAAH ASPEK PERLINDUNGAN KORBAN* DALAM HUKUM NASIONAL

Yang, M. (2025). Urgensi formulasi perlindungan hukum dan kepastian pidana terhadap pengaturan tindak pidana *deepfake* dalam sistem hukum pidana nasional. *Rewang Rencang: Jurnal Hukum Lex Generalis*, 6(7), 3.

## Website

Castro, D. (2020) 'Deepfakes Are on the Rise — How Should Government Respond?', *GovTech*. URL: <https://www.govtech.com/policy/deepfakes-are-on-the-rise-how-should-government-respond.html> (Diakses 29 November 2025).

CNN Indonesia (2025) 'Modus penipuan deepfake AI, Prabowo-Gibran tawarkan bantuan uang', *CNN Indonesia*, 24 Januari. URL: <https://www.cnnindonesia.com/nasional/20250124072755-12-1190915/modus-penipuan-deepfake-ai-prabowo-gibran-tawarkan-bantuan-uang> (Diakses 29 November 2025)

kumparanNEWS (2025) 'Terungkapnya Kasus Konten Porno Deepfake Mahasiswi Unud', *kumparan.com*, 27 April. URL: <https://kumparan.com/kumparannews/terungkapnya-kasus-konten-porno-deepfake-mahasiswi-unud-24xOaAR2Ntv> (Diakses 29 November 2025).

Zhang, L. (2023) 'China: Provisions on Deep Synthesis Technology Enter into Effect', *Global Legal Monitor / Library of Congress*, 25 April. URL: <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/> (Diakses 29 November 2025).

## Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban

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

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

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

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua  
Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi  
Elektronik