

Pertanggungjawaban Pidana terhadap Penyalahgunaan Teknologi *Deepfake* Sebagai Bentuk Kejahatan Digital

Afifah Devi Nabilah, Arga Chon Feriandref, Othman Ballan

Universitas Graha Karya Muara Bulian

Correspondence email: afifahdevinabilah@gmail.com, argaandref@gmail.com, othmanballan84@gmail.com

Article Info	Abstract
Keywords: <i>Deepfake, Criminal Liability, Digital Crime, Technology, Criminal Law</i> Submitted: 26-08-2026 Revised: 18-09-2026 Accepted: 24-10-2026 Published: 25-10-2026	<i>The development of digital technology and artificial intelligence has led to the emergence of deepfake technology, which is capable of creating or manipulating digital content in the form of images, videos, and audio to appear authentic. The ease of using this technology has created legal problems when deepfakes is misused as a means of committing digital crimes, such as fraud, defamation, information manipulation, and the distribution of harmful content. This study aims to analyze the forms of deepfake technology misuse as digital crimes and examine the criminal liability of perpetrators under Indonesian criminal law. This research employs a normative juridical method using a statutory approach and a conceptual approach. The results indicate that although there is currently no specific criminal provision regulating the misuse of deepfake technology, such acts may still give rise to criminal liability insofar as the elements of an offense regulated under existing legislation are fulfilled. Criminal liability may be imposed based in the nature of the unlawful act and its consequences, taking into account the existence of an unlawful act, the perpetrator's culpability, criminal capacity and the absence of justifying or excusing grounds. Therefore, the development of deepfake technology needs to be accompanied by the strengthening and reform of criminal law to provide more effective legal protection for society against various forms of digital crime.</i>
	Abstrak
Kata Kunci: <i>Deepfake, Pertanggungjawaban Pidana, Kejahatan Digital, Teknologi, Hukum Pidana</i>	Perkembangan teknologi digital dan kecerdasan buatan telah melahirkan teknologi <i>deepfake</i> yang mampu menghasilkan atau memanipulasi konten digital berupa gambar, video, maupun suara sehingga menyerupai keadaan yang sebenarnya. Kemudahan penggunaan teknologi tersebut menimbulkan persoalan hukum ketika <i>deepfake</i> disalahgunakan sebagai sarana melakukan kejahatan digital, seperti penipuan, pencemaran nama baik, manipulasi informasi, dan penyebaran konten yang merugikan orang lain. Penelitian ini bertujuan untuk menganalisis bentuk pertanggungjawaban penyalahgunaan teknologi <i>deepfake</i> sebagai kejahatan digital dalam hukum pidana Indonesia. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian ini menunjukkan bahwa data pribadi anak merupakan bagian dari hak privasi yang memperoleh perlindungan meskipun belum terdapat ketentuan pidana yang secara khusus mengatur mengenai penyalahgunaan teknologi <i>deepfake</i>, yang telah diatur dalam peraturan perundang-undangan. Pertanggungjawaban pidana dapat dikenakan berdasarkan jenis perbuatan dan akibat yang ditimbulkan, dengan memperhatikan adanya perbuatan melawan hukum, kesalahan pelaku, kemampuan bertanggung jawab. Dengan demikian, perkembangan teknologi <i>deepfake</i> perlu diikuti dengan penguatan dan pembaruan hukum pidana agar mampu memberikan perlindungan hukum yang lebih efektif terhadap masyarakat dari berbagai bentuk kejahatan digital.

PENDAHULUAN

Perkembangan teknologi digital dan kecerdasan buatan (*Artificial Intelligence/AI*) telah membawa perubahan yang semakin luas dalam kehidupan masyarakat, termasuk dalam menghasilkan dan memanipulasi berbagai bentuk konten digital. Salah satu perkembangan yang muncul dari kemajuan tersebut adalah teknologi *deepfake*, yaitu teknologi yang memungkinkan penciptaan atau perubahan gambar, suara, maupun video dengan tingkat kemiripan yang tinggi terhadap kondisi

sebenarnya.¹ Kehadiran teknologi ini oada dasarnya dapat memberikan manfaat dalam berbagai bidang, tetapi kemampuan untuk menghasilkan konten yang menyerupai kenyataan juga membuka peluang bagi penggunaannya secara tidak bertanggungjawab. Ketika teknologi *deepfake* digunakan sebagai sarana untuk melakukan perbuatan yang merugikan orang lain, persoalannya tidak lagi terbatas pada perkembangan teknologi, tetapi telah memasuki ranah hukum pidana.

Penyalahgunaan *deepfake* dapat digunakan untuk membuat seseorang seolah-olah melakukan tindakan atau mengucapkan pernyataan yang sebenarnya tidak pernah dilakukan atau disampaikan. Kondisi tersebut dapat dimanfaatkan untuk melakukan penipuan, pemalsuan identitas, pencemaran nama baik, pemerasan, penyebaran informasi palsu, hingga pembuatan konten seksual tanpa persetujuan pihak yang bersangkutan. Karakteristik *deepfake* yang mampu menghasilkan konten menyerupai kenyataan menyebabkan perbuatan tersebut berpotensi menimbulkan kerugian yang serius bagi korban. Selain kerugian materiil, penyalahgunaan identitas melalui *deepfake* dapat mengganggu kehormatan, reputasi, serta keamanan seseorang dalam ruang digital. Dalam sistem peradilan pidana juga terlihat bahwa *deepfake* sebagai bentuk perkembangan teknologi dapat menimbulkan tantangan terhadap proses penegakan hukum karena semakin sulitnya membedakan antara konten yang autentik dan konten yang telah dimanipulasi.²

Persoalan yang kemudian muncul bukan hanya mengenai adanya perbuatan yang merugikan, tetapi juga mengenai pihak yang dapat dimintai pertanggungjawaban atas perbuatan tersebut. dalam tindak pidana yang memanfaatkan *deepfake*, teknologi kecerdasan buatan digunakan sebagai instrumen untuk menghasilkan suatu konten, sedangkan tindakan tersebut tetap berasal dari keputusan dan kehendak manusia yang mengoperasikannya atau memanfaatkannya. Keadaan ini menimbulkan persoalan dalam menentukan hubungan antara penggunaan teknologi, perbuatan pidana, dan pihak yang harus mempertanggungjawabkan akibat yang ditimbulkan. Terlebih lagi, suatu konten *deepfake* dapat dibuat oleh satu pihak dan kemudian disebarluaskan oleh pihak lainnya. Perbedaan peran tersebut menyebabkan penentuan pihak yang bertanggung jawab tidak dapat dilakukan hanya dengan melihat siapa yang pertama kali menghasilkan konten, tetapi perlu memperhatikan keterlibatan masing-masing pihak dalam terjadinya tindak pidana.

Permasalahan pertanggungjawaban pidana menjadi semakin penting karena penggunaan teknologi tidak serta-merta menghilangkan tanggung jawab manusia atas suatu perbuatan pidana. dalam konteks *deepfake*, perlu diketahui apakah seseorang yang menggunakan teknologi tersebut memiliki kesengajaan untuk melakukan perbuatan yang dilarang, mengetahui akibat dari tindakannya, atau dengan sengaja membiarkan teknologi tersebut digunakan untuk mencapai tujuan tertentu. Penentuan pertanggungjawaban juga berkaitan dengan kemampuan untuk menghubungkan perbuatan pelaku dengan akibat yang ditimbulkan terhadap korban. Oleh karena itu, penggunaan teknologi kecerdasan buatan sebagai sarana kejahatan tidak seharusnya dipandang sebagai keadaan yang secara otomatis memindahkan tanggung jawab kepada teknologi, melainkan perlu diterlusrui berdasarkan peran, tindakan dan kesalahan dari pihak yang menggunakan.

Perkembangan *deepfake* juga memperlihatkan adanya persoalan baru dalam menentukan subjek yang bertanggung jawab ketika kecerdasan buatan terlibat dalam proses terjadinya tindak pidana. teknologi kecerdasan buatan dapat menjalankan proses tertentu secara otomatis berdasarkan sistem dan data yang digunakan, tetapi teknologi tersebut tidak memiliki kedudukan yang sama dengan manusia sebagai pelaku yang mempunyai kehendak dan kemampuan untuk mempertanggungjawabkan perbuatannya. Perkembangan pemikiran mengenai pertanggungjawaban pidana dalam kejahatan *deepfake* juga menunjukkan bahwa kesalahan dan pihak yang mengendalikan penggunaan teknologi menjadi bagian penting dalam menentukan konstruksi pertanggungjawaban pidananya.³

Selain persoalan terkait subjek yang dapat dimintai pertanggungjawabbaan, penyalahgunaan *deepfake* juga menimbulkan persoalan dalam membuktikan keterlibatan dan kesalahan pelaku. Karakteristik teknologi yang memungkinkan pembuatan konten secara cepat dan mudah dapat

¹Maria-Paz Sandoval, "Threat of Deepfake to the Criminal Justice System: A Systematic Review", *Crime Science, Volume 13, Nomor 41*, (2024): 20.

²Asri Gresmelian and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia", *Asian Journal of Social and Humanities, Volume 2, Nomor 4*, (2024): 777.

³Muhammad Syafiq, "Artificial Intelligence-Based Deepfake Crimes: A Conception Of Culpability Principle As A Criminal Liability Reform", *Reformasi Hukum, Volume 29, Nomor 2*, (2025): 59.

menyebabkan identitas pembuat maupun pihak yang menyebarkan konten sulit untuk ditelusuri. Dalam keadaan tertentu, pelaku dapat menggunakan berbagai akun atau sarana digital untuk menyembunyikan identitasnya, sementara konten yang telah dibuat dapat disebarluaskan oleh pihak lain tanpa keterlibatan langsung dari pembuat awal. Kondisi tersebut menjadikan proses penentuan hubungan antara pelaku dan tindak pidana sebagai bagian yang penting dalam menentukan pertanggungjawaban pidana.

Di samping itu, perkembangan penggunaan *deepfake* menunjukkan bahwa pertanggungjawaban pidana perlu ditempatkan secara proporsional terhadap peran masing-masing pihak. Seseorang yang dengan sengaja membuat *deepfake* untuk melakukan tindak pidana memiliki posisi yang berbeda dengan pihak yang secara tidak sengaja menerima atau menyebarkan konten tersebut tanpa mengetahui bahwa konten tersebut merupakan hasil manipulasi. Demikian pula, pihak yang hanya menjadi korban manipulasi tidak dapat dipersamakan dengan pihak yang secara sadar menggunakan teknologi tersebut untuk memperoleh keuntungan atau menimbulkan kerugian bagi orang lain. Perbedaan keadaan tersebut penting diperhatikan agar penentuan pertanggungjawaban pidana tidak hanya didasarkan pada keterlibatan seseorang terhadap suatu konten, tetapi juga mempertimbangkan pengetahuan, kehendak, tujuan, serta bentuk kesalahan yang menyertai perbuatannya. Dengan demikian, penggunaan teknologi *deepfake* sebagai sarana kejahatan tetap dapat ditempatkan dalam kerangka pertanggungjawaban pidana yang berorientasi pada perbuatan dan kesalahan pelaku.

Persoalan tersebut menempatkan pertanggungjawaban pidana sebagai aspek yang penting untuk dikaji dalam penyalahgunaan teknologi *deepfake*. Keberadaan teknologi sebagai sarana melakukan tindak pidana tidak menghapus kebutuhan untuk menentukan siapa yang harus mempertanggungjawabkan perbuatan tersebut, bagaimana hubungan pelaku dengan perbuatan yang dilakukan, serta apakah terdapat kesalahan yang dapat menjadi dasar pemidanaan. Hal ini diperlukan agar perkembangan teknologi tidak menciptakan ruang bagi pelaku untuk menghindari pertanggungjawaban dengan menjadikan kecerdasan buatan sebagai alasan atas perbuatan yang dilakukannya. Persoalan terkait subjek yang bertanggungjawab, bentuk keterlibatan, serta kesalahan dalam penggunaan *deepfake* menjadi dasar penting untuk mengkaji pertanggungjawaban pidana dalam perkembangan kejahatan digital yang memfokuskan pembahasan pada aspek yang dapat dimintai pertanggungjawaban pidana dan dasar pertanggungjawaban pidana atas penggunaan teknologi *deepfake* dalam melakukan tindak pidana.

METODE

1. Pendekatan

Mengingat penelitian tentang pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* sebagai bentuk kejahatan digital merupakan penelitian yuridis normatif yaitu penelitian yang menempatkan hukum sebagai suatu sistem norma yang dikaji melalui peraturan perundang-undangan, doktrin, asas hukum, dan berbagai literatur yang relevan dengan isu hukum yang diteliti.⁴ Dengan pendekatan yang digunakan dalam penelitian ini adalah pendekatan undang-undang (*statute approach*) dan pendekatan konseptual (*conceptual approach*).⁵ Pendekatan perundang-undangan digunakan untuk menelaah berbagai ketentuan hukum yang berkaitan dengan penyalahgunaan teknologi digital, tindak pidana, serta pertanggungjawaban pidana. Sementara itu, pendekatan konseptual digunakan untuk memahami konsep pertanggungjawaban pidana, kesalahan, kemampuan bertanggung jawab, serta konsep kejahatan digital yang berkaitan dengan penyalahgunaan teknologi *deepfake*. Dengan menggunakan pendekatan perundang-undangan, peneliti menelaah berbagai peraturan perundang-undangan yang memiliki relevansi dengan penyalahgunaan teknologi *deepfake* dan pertanggungjawaban pidana pelakunya. Peraturan menjadi dasar analisis antara lain Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta peraturan perundang-undangan lain yang berkaitan dengan perlindungan data pribadi, penghinaan, pencemaran nama baik, pemalsuan, penipuan maupun bentuk tindak pidana digital lainnya. Selain itu, pendekatan konseptual digunakan untuk

⁴Sidi Ahyia Wiraguna, "Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia", *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum*, Volume 3, Nomor 3, (2024): 59.

⁵ Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum* (Bandung: Mandar Maju, 2008), hlm.87.

- menganalisis bagaimana konsep pertanggung jawaban pidana dapat diterapkan terhadap pelaku penyalahgunaan teknologi *deepfake*.
2. Rancangan Kegiatan

Dalam rangka melakukan penleitian yang mendalam mengenai pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* sebagai bentuk kejahatan digital, disusun rencana kegiatan penelitian yang meliputi beberapa tahapan. Tahapan tersebut dimulai dari identifikasi permasalahan, studi kepustakaan, pengumpulan bahan hukum. Penelaahan peraturan perundang-undangan dan literatur yang relevan, hingga analisis terhadap bentuk penyalahgunaan teknologi *deepfake* dan pertanggungjawaban pidana terhadap pelakunya.
 3. Ruang Lingkup atau Objek

Ruang lingkup dan objek penleitian ini mencakup penyalahgunaan teknologi *deepfake* sebagai sarana melakukan tindak pidana digital serta bentuk pertanggungjawaban pidana terhadap pihak yang menyalahgunakan teknologi tersebut. penelitian difokuskan pada berbagai bentuk penyalahgunaan *deepfake* yang dapat menimbulkan akibat hukum, seperti manipulasi gambar, video, atau suara seseorang yang digunakan untuk melakukan penipuan, pencemaran nama baik, penyebaran informasi palsu, pemalsuan identitas, maupun perbuatan lain yang memenuhi unsur tindak pidana. selain itu, penlitian ini juga mengkaji unsur-unsur pertanggungjawaban pidana terhaadap pelaku penyalahgunaan *deepfake*, meliputi adanya perbuatan pidana, kemampuan bertanggung jawab, adanya kesalahan dalam bentuk kesengajaan atau kealpaan. Ruang lingkup penelitian juga mencakup penerapan ketentuan hukum pidana yang berlaku terhadap perbuatan penyalahgunaan teknologi *deepfake*.
 4. Bahan dan Alat Utama
 - a. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hokum yang memiliki kekuat mengikat dan menjadi dasar utama dalam penlitian hkum normatif. Bahan hukum primer dalam penleitian ini meliputi peraturan perundang-undangan yang berkaitan dengan tindak pidana dan pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake*.
 - b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan yang memberikan penjelasan dan pendapat terhadap bahan hkum primer. Bahan hukom sekunder yang digunakan dalam penleitian ini meliputi buku-buku hukum pidana, buku mengenai hukum siber dan kejahatan siber dan kejahatan digital, jurnal ilmiah, artikel ilmiah, hasil penelitian dan pendapat para ahli yang berkaitan dengan pertanggungjwaaban pidana, teknologi *deepfake*, dan kejahatan digital. Bahan hukum sekunder ini digunakan untuk memberikan pemahaman teoritis dan konseptual dalam menganalisis penerapan pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake*.
 - c. Bahan Hukum Tersier

Bahan hukum tersier merupakan bahaan yang digunakan untuk menunjukkan maupun menjelaskan terhdap bahan hokum primer dan sekunder. Bahan hokum tersier dalam penlitian ini dapat berupa Kamus Besar Bahasa Indonesia, kamus hukum, serta sumber refherensi lainnya yang dapat membantu memherjelas istilah dan konsep yang berkaitan dengan teknologi *deepfake*, tindak pidana, kejahatan digital, dan pertanggungjwaban pidana.
 5. Tempat

Penelitian ini tidak dilakukan pada lokasi tertentu karena merupakan pnelitian yuridis normatif yang menggunakan studi kepustakaan. Tempat dalam penelitian ini merujuk pada wilayah hukum Indonesia, mengingat objek kajian berkaitan dengan penerapan ketentuan hukum pidana Indonesia terhadap penyalahgunaan teknologi *deepfake* sebagai bentuk kejahatan digital.
 6. Teknik Pengumpulan Data

Teknik pengmpulan bahan hukum dalam peneleitian ini dilakukan melalui studi kepustakaan dan studi dokumen. Studi kepustakaan dilakukan dngan mengumpulkan dan mempelajari berbagai bahan hkum primer, sekunder dan tersier yang memiliki relevansi dengan pertanggungjawaban pidana dan penyalahgunaan teknologi *deepfake*. Bahan hukum tersebut diperoleh melalui penelusuran peraturan perundang-undangan, buku, jurnal ilmiah, artikel, hasil penelitian dan lain sebagainya. Studi dokumen dilakukan dengan menelaah dokumen-dokumen hukum yang berkaitan

dengan objek penelitian untuk memperoleh pemahaman mengenai ketentuan hukum yang dapat diterapkan terhadap penyalahgunaan teknologi *deepfake*.

7. Definisi Operasional Variabel Penelitian

a. Pertanggungjawaban Pidana

Pertanggungjawaban pidana merupakan bentuk pertanggungjawaban seseorang atas perbuatan pidana yang dilakukannya berdasarkan adanya kesalahan yang dapat dibebankan kepada pelaku. Pertanggungjawaban pidana dalam penelitian ini berkaitan dengan kemampuan pelaku penyalahgunaan teknologi *deepfake* untuk mempertanggungjawabkan perbuatannya menurut hukum pidana, dengan memperhatikan unsur kesalahan, kemampuan bertanggungjawab.

b. Penyalahgunaan Teknologi *Deepfake*

Penyalahgunaan teknologi *deepfake* adalah penggunaan teknologi kecerdasan buatan untuk membuat atau memanipulasi gambar, video, suara, maupun bentuk media digital lainnya sehingga menyerupai keadaan atau identitas seorang secara tidak benar dan digunakan untuk tujuan yang melanggar hukum.

c. Kejahatan Digital

Kejahatan digital merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi informasi, perangkat elektronik, jaringan internet, atau media digital sebagai sarana, sasaran, maupun pendukung terjadinya suatu tindak pidana.

8. Teknik Analisis

Penelitian mengenai pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* sebagai bentuk kejahatan digital menggunakan teknik analisis kualitatif. Analisis dilakukan dengan cara menguraikan, menafsirkan, dan menghubungkan bahan hukum yang telah dikumpulkan dengan permasalahan penelitian. Analisis tersebut diarahkan untuk mengidentifikasi bentuk-bentuk penyalahgunaan teknologi *deepfake* yang dapat dikategorikan sebagai tindak pidana digital serta menentukan dasar dan bentuk pertanggungjawaban pidana terhadap pelakunya. Dengan demikian, analisis dilakukan untuk memperoleh gambaran mengenai penerapan hukum pidana terhadap penyalahgunaan teknologi *deepfake* serta sejauh mana ketentuan hukum yang berlaku dapat digunakan untuk membebaskan pertanggungjawaban pidana pidana kepada pelaku.

HASIL

Bentuk Penyalahgunaan Teknologi *Deepfake* Sebagai Sarana Tindak Pidana Digital

Perkembangan teknologi digital dan kecerdasan buatan telah membawa perubahan yang signifikan terhadap cara manusia menghasilkan, mengolah, dan menyebarkan informasi. Salah satu perkembangan tersebut adalah teknologi *deepfake*, yang pada dasarnya dapat digunakan untuk menghasilkan atau memanipulasi konten digital dengan tingkat kemiripan yang tinggi terhadap kondisi sebenarnya. Dalam konteks kejahatan digital, kemampuan tersebut menjadi persoalan ketika teknologi *deepfake* digunakan untuk menciptakan informasi atau representasi seseorang yang tidak sesuai dengan kenyataan, sehingga dapat digunakan sebagai sarana untuk melakukan perbuatan yang merugikan pihak lain.

Secara karakteristik, *deepfake* merupakan teknologi yang memanfaatkan kecerdasan buatan, khususnya metode *deep learning*, untuk menghasilkan atau memanipulasi media digital berupa gambar, video, maupun suara. Proses tersebut memungkinkan suatu konten yang semula autentik diubah dengan memasukkan atau menggantikan unsur tertentu sehingga menghasilkan tampilan atau suara yang menyerupai orang dan keadaan sebenarnya. *Deepfake* itu sendiri dapat menghasilkan gambar, video, dan audio yang bersifat artifisial tetapi memiliki tingkat kemiripan yang sangat tinggi dengan kenyataan.⁶ Karakteristik inilah yang membedakan *deepfake* dari manipulasi digital sederhana, karena perubahan yang dihasilkan tidak hanya bersifat visual, tetapi dapat membentuk suatu representasi yang seolah-olah benar-benar pernah terjadi.

Pada media gambar dan video, manipulasi *deepfake* dapat dilakukan dengan mengubah identitas atau karakteristik wajah seseorang, termasuk menggantikan wajah seseorang dengan wajah orang lain. Teknologi tersebut juga dapat digunakan untuk menghasilkan ekspresi atau gerakan wajah tertentu sehingga seseorang tampak melakukan atau mengatakan sesuatu yang sebenarnya tidak pernah

⁶Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara", *Jurnal USM Law Review*, Volume 7, Nomor 2, (2024): 604, doi.org

dilakukan. Perkembangan metode *deep learning* telah memungkinkan terbentuknya video *deepfake* yang sangat realistis, termasuk melalui teknik pertukaran wajah (*face swapping*).⁷ Dengan demikian, karakteristik utama pada manipulasi visual terletak pada kemampuan teknologi untuk mempertahankan konteks visual suatu rekaman sekaligus mengubah identitas atau tindakan subjek di dalamnya.

Selain gambar dan video, *deepfake* juga dapat diterapkan terhadap data suara. Manipulasi suara memungkinkan karakteristik suara seseorang ditiru atau direkayasa sehingga suara yang dihasilkan terdengar terdengar seperti suara individu tertentu. Perkembangan *machine learning* telah menghasilkan *deepfake* pada ranah visual maupun audio yang semakin sulit dibedakan dari media asli.⁸ Dalam konteks kejahatan digital, karakteristik ini menjadi penting karena suara seseorang dapat digunakan sebagai representasi identitas, sehingga rekayasa suara dapat menciptakan kesan seolah-olah seseorang benar-benar menyampaikan suatu pernyataan atau memberikan suatu perintah.

Karakteristik lain yang menonjol dari penyalahgunaan *deepfake* adalah tingkat kemiripan dan daya meyakinkan yang dihasilkan. Teknologi ini tidak sekadar menghasilkan konten yang tampak palsu, melainkan berupaya menghasilkan media yang menyerupai keadaan nyata sehingga penerima informasi dapat mengalami kesulitan dalam membedakannya dari konten autentik. Peningkatan kualitas dan daya persuasif *deepfake* memperbesar potensi manipulasi karena perkembangan kecerdasan buatan telah mempermudah serta meningkatkan kualitas proses manipulasi dan sintesis audio, video, maupun gambar.⁹ Oleh karena itu, konteks kejahatan digital, persoalan utama *deepfake* tidak hanya terletak pada adanya perubahan terhadap suatu konten, tetapi juga pada kemampuan perubahan tersebut untuk menciptakan persepsi mengenai suatu peristiwa yang sebenarnya tidak pernah terjadi.

Penyalahgunaan *deepfake* juga memiliki karakteristik berupa kemampuan menggabungkan beberapa unsur media secara bersamaan. Sebuah video, misalnya, dapat memuat manipulasi wajah sekaligus suara yang dibuat menyerupai individu tertentu sehingga menghasilkan representasi yang semakin meyakinkan. Kondisi tersebut menunjukkan bahwa *deepfake* dapat bekerja secara multimodal, yaitu memanipulasi lebih dari satu jenis informasi digital dalam suatu konten. Perkembangan tersebut semakin memperbesar kesulitan dalam membedakan konten asli dan konten hasil manipulasi, terutama proses penyebaran.¹⁰

Berdasarkan karakteristik tersebut, penyalahgunaan teknologi *deepfake* sebagai sarana tindak pidana digital pada dasarnya dapat dipahami sebagai penggunaan teknologi kecerdasan buatan untuk menciptakan atau memodifikasi representasi digital seseorang atau suatu keadaan agar tampak autentik, padahal tidak sesuai dengan kenyataan. Manipulasi tersebut dapat menysar gambar, video, suara, maupun kombinasi beberapa media sekaligus. Karakteristik berupa kemampuan menghasilkan konten yang realistis, menyerupai identitas seseorang, serta sulit dibedakan dari keadaan sebenarnya menjadikan *deepfake* memiliki potensi untuk digunakan sebagai instrumen dalam berbagai bentuk kejahatan digital. Berikut adalah uraian tentang bentuk penyalahgunaan *deepfake* sebagai sarana tindak pidana digital dapat dikelompokkan berdasarkan tujuan atau cara penggunaannya, yaitu:

1. Penipuan

Pelaku dapat memanfaatkan wajah atau suara seseorang yang dikenal korban untuk menciptakan komunikasi atau tampilan seolah-olah berasal dari orang yang sebenarnya. Manipulasi tersebut dapat digunakan untuk meyakinkan korban agar memberikan sejumlah uang, data pribadi atau melakukan tindakan tertentu. Terdapat beberapa kasus terkait penipuan yang dilakukan melalui *deepfake*, salah satu kasus nyata yang terjadi di Indonesia, teknologi *deepfake* bahkan telah digunakan dengan memanfaatkan wajah dan suara Baim Wong untuk mengelabui korban melalui modus pemberian hadiah. Peristiwa tersebut menunjukkan bahwa *deepfake* dapat memperkuat

⁷Fasa Muhamad Hapid, dkk, "Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake", *Jurnal USM Law Review*, Volume 7, Nomor 3, (2024): 1156, <https://journals.usm.ac.id/index.php/julr/article/view/9686>

⁸Supuan Sultan Al-Alif dan Cik Marhayati, "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake Di Indonesia", *Legal Standing: Jurnal Ilmu Hukum*, Volume 9, Nomor 5, (2025): 1170.

⁹*Ibid.*

¹⁰Aisya Alyani adalah Aisya Alyani, "Dampak Penyalahgunaan Deepfake Dalam Memanipulasi Visual: Menguak Potensi Infopocalypse Di Era Post Truth Terhadap Asumsi Masyarakat Pada Media Massa", *Jurnal Kawistara*, Volume 14, Nomor 3, (2024): 408.

modus penipuan karena pelaku tidak hanya mengandalkan komunikasi tertulis atau suara, tetapi juga menghadirkan representasi visual yang membuat identitas palsu terlihat lebih meyakinkan.¹¹

2. Pemalsuan atau penyalahgunaan identitas

Dalam praktiknya, pelaku dapat menggunakan foto, video, maupun rekaman suara seseorang sebagai bahan untuk membentuk identitas digital yang seolah-olah benar. Identitas tersebut kemudian dapat digunakan untuk melakukan komunikasi, membuat pernyataan, atau melakukan suatu tindakan tanpa sepengetahuan pemilik identitas. Penyalahgunaan identitas melalui *deepfake* menjadi semakin berbahaya karena korban bukan hanya kehilangan kendali atas penggunaan representasi dirinya, tetapi juga dapat dikaitkan dengan suatu perbuatan yang tidak pernah dilakukannya. Dengan demikian, penggunaan identitas orang lain melalui teknologi *deepfake* dapat menjadi sarana untuk menyamarkan identitas pelaku sekaligus meyakinkan pihak lain mengenai kebenaran identitas yang ditampilkan.¹²

3. Pencemaran nama baik

Perbuatan tersebut dapat dilakukan dengan menggunakan gambar, video, atau suara yang seolah-olah menunjukkan seseorang melakukan atau mengatakan sesuatu yang dapat merendahkan kehormatan maupun reputasinya. Konten yang telah dimanipulasi kemudian disebarluaskan melalui media digital sehingga dapat diketahui oleh orang lain. Salah satu bentuk konten yang merupakan pencemaran nama baik bisa berupa konten pornografi yang dibuat menggunakan *deepfake* dalam keadaan tertentu dapat dikategorikan sebagai bentuk pencemaran nama baik karena konten tersebut dapat memberikan gambaran yang merendahkan korban dan memenuhi unsur pencemaran sebagaimana diatur dalam hukum pidana.¹³ Oleh sebab itu, penggunaan *deepfake* dalam konteks ini tidak hanya merupakan persoalan manipulasi teknologi, tetapi dapat menjadi sarana untuk menyerang kehormatan dan nama baik seseorang.

4. Pemerasan

Pemerasan dalam hal ini termasuk pemerasan yang menggunakan konten seksual atau intim hasil manipulasi *deepfake*. Pelaku dapat membuat atau menggunakan gambar dan video palsu yang menampilkan korban dalam keadaan intim, kemudian mengancam akan menyebarkan konten tersebut apabila korban tidak memberikan uang atau memenuhi permintaan tertentu. Pola demikian menunjukkan bahwa *deepfake* dapat digunakan sebagai alat tekanan terhadap korban karena pelaku memanfaatkan rasa takut korban terhadap konsekuensi sosial apabila konten tersebut tersebar.¹⁴

5. Penyebaran konten intim tanpa persetujuan

Dalam praktik *deepfake*, pelaku dapat mengambil wajah atau identitas seseorang kemudian menempatkannya pada tubuh orang lain dalam suatu gambar atau video yang bersifat seksual. Korban seolah-olah menjadi pihak yang terdapat dalam konten tersebut, padahal tidak pernah membuat atau menyetujui pembuatannya. Perbuatan tersebut dapat menimbulkan persoalan hukum karena menyangkut penggunaan identitas, privasi, kehormatan, serta penyebaran konten seksual tanpa persetujuan. Literatur hukum nasional juga menunjukkan bahwa pornografi berbasis *deepfake* merupakan salah satu bentuk penyalahgunaan yang berkembang dan memiliki karakteristik berbeda dari pornografi konvensional karena korban dapat dimasukkan ke dalam konten tanpa pernah melakukan tindakan yang ditampilkan.¹⁵

Penyalahgunaan teknologi *deepfake* sebagai sarana tindak pidana digital tidak hanya menimbulkan persoalan terhadap keaslian informasi yang beredar, tetapi juga dapat memberikan dampak langsung kepada pihak yang menjadi sasaran manipulasi. Kemampuan *deepfake* dalam menciptakan gambar, video, atau suara yang menyerupai keadaan sebenarnya menyebabkan korban

¹¹Fasa Muhamad Hapid, dkk, *Op.Cit.*, hlm. 1158.

¹²Chiquita Thefirstly Noerman dan Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara", *Jurnal USM Law Review*, Volume 7, Nomor 2, (2024): 610.

¹³Sarah Amanda U.S., dan Diana Lukitasari, "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik", *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, Volume 13, Nomor 2, (2024): 169.

¹⁴Rio Irandha Putra, "Deepfake Sebagai Sarana Pemerasan Dalam Perspektif Hukum Pidana Indonesia", *Risalah Hukum*, Volume 22, Nomor 1, (2026): 26.

¹⁵Muhammad Faqih dan E.S. Priowirjanto, "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia", *Jurnal Indonesia Sosial Teknologi*, Volume 3, Nomor 11, (2022): 1158.

dapat ditempatkan dalam suatu keadaan yang tidak pernah dilakukan atau dialaminya. Akibatnya, kerugian yang muncul tidak hanya berkaitan dengan kehilangan harta benda, tetapi juga dapat menyentuh aspek pribadi korban, seperti nama baik, kehormatan, privasi, dan rasa aman.

Dari sisi kerugian materiil, penyalahgunaan *deepfake* dapat menyebabkan korban mengalami kehilangan atau kerugian ekonomi secara langsung. Misalnya, ketika identitas, wajah, atau suara korban digunakan untuk melakukan penipuan, pihak lain dapat memberikan uang atau melakukan transaksi berdasarkan representasi palsu yang dibuat pelaku. Korban juga dapat mengalami kerugian ekonomi apabila citra atau identitasnya digunakan untuk kepentingan tertentu tanpa persetujuan, terutama ketika penggunaan tersebut menimbulkan kehilangan kesempatan, gangguan terhadap pekerjaan, atau kerugian terhadap kegiatan ekonomi korban. Dengan demikian, konsekuensi lanjutan dari penggunaan identitas korban secara tidak sah.

Selain kerugian ekonomi, penyalahgunaan *deepfake* dapat menimbulkan kerugian terhadap nama baik dan kehormatan korban. Manipulasi gambar, video, atau suara dapat membuat korban seolah-olah melakukan perbuatan tertentu yang bertentangan dengan kenyataan. Ketika konten tersebut disebarluaskan melalui media digital, informasi palsu tersebut dapat diketahui oleh masyarakat dalam jumlah luas dan menyebar dengan cepat. Keadaan tersebut berpotensi membentuk persepsi negatif terhadap korban sebelum kebenaran mengenai konten tersebut diketahui. Dalam konteks pencemaran nama baik, penggunaan teknologi *deepfake* menjadi semakin berisiko karena konten yang dimanipulasi dapat memiliki tampilan yang meyakinkan sehingga orang lain dapat mempercayainya sebagai keadaan yang benar.¹⁶

Dampak lainnya berkaitan dengan privasi, keamanan dan kondisi psikologis korban. Penggunaan foto, video, atau suara seseorang tanpa persetujuan menunjukkan bahwa korban kehilangan kendali atas representasi dirinya di ruang digital. Kondisi tersebut dapat semakin serius apabila *deepfake* digunakan untuk menghasilkan konten intim atau pornografi, karena korban dapat mengalami rasa malu, tekanan sosial, ketakutan terhadap penyebaran konten, serta gangguan terhadap kehidupan pribadi.¹⁷ Penyalahgunaan *deepfake* pornografi, dampak yang ditimbulkan dapat meluas pada aspek psikologis, sosial, dan reputasional korban.¹⁸

Berdasarkan uraian penjelasan diatas, dapat dipahami bahwa teknologi *deepfake* telah berkembang menjadi sarana yang dapat memperkuat pelaksanaan berbagai tindak pidana digital. Kemampuannya dalam menghasilkan manipulasi gambar, video, dan suara yang menyerupai keadaan sebenarnya memungkinkan pelaku melakukan penipuan, penyalahgunaan identitas, pencemaran nama baik, pemerasan, hingga penyebaran konten intim tanpa persetujuan, yang pada akhirnya dapat menimbulkan kerugian materiil, maupun immateriil bagi korban. Kondisi tersebut menunjukkan bahwa penyalahgunaan *deepfake* bukan semata-mata persoalan perkembangan teknologi, melainkan telah menjadi persoalan hukum pidana karena dapat digunakan untuk melakukan perbuatan yang merugikan kepentingan dan hak seseorang.

Pertanggungjawaban Pidana Terhadap Penyalahgunaan Teknologi Deepfake Sebagai Tindak Pidana Digital

Pertanggungjawaban pidana pada dasarnya tidak hanya didasarkan pada terbuktinya suatu perbuatan sebagai tindak pidana, tetapi juga mensyaratkan bahwa orang yang melakukan perbuatan tersebut memiliki kemampuan untuk mempertanggungjawabkan perbuatannya. Kemampuan bertanggung jawab berkaitan dengan keadaan diri pelaku pada saat tindak pidana dilakukan, khususnya kemampuan untuk memahami makna dan akibat dari perbuatannya serta menentukan kehendaknya terhadap perbuatan tersebut. dalam konteks penyalahgunaan teknologi *deepfake*, persoalan kemampuan bertanggung jawab menjadi penting karena teknologi tersebut digunakan sebagai sarana dalam melakukan suatu tindak pidana, sehingga menjadi subjek penilaian pertanggungjawaban pidana, sehingga menjadi subjek penilaian pertanggungjawaban pidana adalah orang yang menggunakan atau memanfaatkan teknologi tersebut untuk melakukan perbuatan yang dilarang oleh hukum.

¹⁶Ni Putu Martina Putri, M.S. Hartono, dan I Dewa Gede H.Y., "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence", *Jurnal Pacta Sunt Servanda*, Volume 5, Nomor 2, (2024): 123.

¹⁷*Ibid.*, hlm. 124.

¹⁸Muhammad Faqih dan E.S. Priowirjanto, *Op.Cit.*, hlm. 1159.

Kemampuan bertanggung jawab pada dasarnya berkaitan dengan keadaan batin pelaku yang memungkinkan dirinya memahami makna dari perbuatan yang dilakukan serta mengendalikan kehendaknya ketika melakukan perbuatan tersebut. Oleh karena itu, seseorang yang menggunakan teknologi *deepfake* tidak serta merta dapat dimintai pertanggungjawaban hanya karena terdapat konten hasil manipulasi yang berkaitan dengannya. Harus dilihat terlebih dahulu apakah orang tersebut mempunyai kemampuan untuk memahami dan mengendalikan perbuatannya pada saat tindak pidana dilakukan. Dalam konteks penyalahgunaan *deepfake*, kemampuan tersebut dapat tercermin dari adanya kemampuan pelaku untuk menggunakan perangkat atau aplikasi, memilih bahan yang akan dimanipulasi, menentukan bentuk manipulasi, serta melakukan tindakan yang berkaitan dengan penyebaran atau penggunaan hasil manipulasi tersebut.¹⁹

Perkembangan hukum pidana Indonesia melalui Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) memberikan pengaturan yang lebih jelas mengenai kemampuan bertanggung jawab. Pasal 38 mengatur bahwa setiap orang yang pada waktu melakukan tindak pidana menyandang disabilitas mental dan/atau disabilitas intelektual dapat dikurangi pidana dan/atau dikenai tindakan. Ketentuan tersebut menunjukkan bahwa kondisi kejiwaan pelaku harus diperhatikan dalam menentukan kemampuan bertanggung jawab dan tidak dapat dinilai hanya berdasarkan fakta bahwa suatu tindak pidana telah terjadi.

Ketentuan tersebut penting diterapkan secara hati-hati dalam perkara penyalahgunaan teknologi *deepfake*. Penggunaan teknologi yang relatif kompleks dalam membuat suatu konten *deepfake* pada dasarnya dapat menjadi salah satu keadaan faktual yang menunjukkan adanya kemampuan pelaku untuk memahami dan mengendalikan tindakan yang dilakukannya, tetapi hal tersebut bukan satu-satunya dasar untuk menyimpulkan kemampuan bertanggung jawab. Penilaian tetap harus diarahkan pada kondisi pelaku pada saat perbuatan itu dilakukan. Dengan demikian, apabila tidak terdapat keadaan yang menunjukkan adanya gangguan terhadap kemampuan pelaku untuk memahami sifat perbuatannya atau mengendalikan kehendaknya, maka pelaku pada prinsipnya dapat dinilai memiliki kemampuan bertanggung jawab. Sebaliknya, apabila terdapat dugaan kondisi kejiwaan yang memengaruhi kemampuan tersebut, pemeriksaan terhadap kondisi pelaku menjadi penting dalam proses penegakan hukum.

Dalam kaitannya dengan penyalahgunaan *deepfake*, kemampuan bertanggungjawab dapat dilihat melalui beberapa keadaan yang relevan, yaitu:

1. Kemampuan memahami perbuatan, yaitu kemampuan pelaku untuk mengetahui bahwa tindakan membuat, menggunakan, atau menyebarkan konten *deepfake* merupakan perbuatan yang dilakukan sendiri dan memiliki konsekuensi tertentu.
2. Kemampuan mengendalikan kehendak, yaitu kemampuan pelaku untuk menentukan dan mengendalikan tindakannya ketika menggunakan teknologi *deepfake*, termasuk ketika memilih untuk membuat atau menyebarkan hasil manipulasi.
3. Keadaan kejiwaan pada saat perbuatan dilakukan, yaitu keadaan mental atau intelektual pelaku ketika tindak pidana berlangsung.

Dengan demikian, dalam penyalahgunaan teknologi *deepfake*, kemampuan bertanggung jawab harus ditempatkan sebagai persoalan mengenai kapasitas pelaku sebagai manusia yang mengendalikan penggunaan teknologi, bukan mengenai kemampuan teknologi kecerdasan buatan itu sendiri. *Deepfake* hanyalah sarana yang digunakan untuk menghasilkan atau memanipulasi konten digital, sedangkan pertanggungjawaban pidana tetap diarahkan kepada manusia yang menggunakan sarana tersebut untuk melakukan tindak pidana. Hal ini sejalan dengan kajian mengenai penyalahgunaan *deepfake* yang menegaskan bahwa penerapan asas *geen zonder schuld* dapat digunakan untuk menentukan apakah seseorang dapat dimintai pertanggungjawaban pidana atas penyalahgunaan teknologi tersebut.

Kemampuan bertanggung jawab dalam penyalahgunaan teknologi *deepfake* pada prinsipnya dapat dinilai apabila pelaku memiliki kapasitas untuk memahami dan mengendalikan perbuatannya serta tidak berada dalam kondisi yang menurut hukum menghilangkan atau mengurangi kemampuan tersebut. Penilaian ini menjadi tahap penting sebelum seseorang dibebani pertanggungjawaban pidana, karena keberadaan suatu perbuatan pidana saja belum cukup untuk membenarkan pemidanaan terhadap pelaku. Dengan demikian, dalam perkara penyalahgunaan *deepfake*, pemeriksaan terhadap kemampuan bertanggungjawab diperlukan untuk memastikan bahwa pertanggungjawaban pidana benar-benar

¹⁹Fasa Muhamad Hapid, dkk, *Op.Cit.*, hlm. 1158.

dibebankan kepada pihak yang secara sadar dan mampu mengendalikan perbuatannya, sesuai dengan prinsip dasar pertanggungjawaban pidana dalam hukum Indonesia.

Pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* tidak cukup hanya didasarkan pada terbuktinya penggunaan teknologi tersebut untuk menghasilkan suatu konten yang merugikan. Dalam hukum pidana, perlu pula dilihat adanya kesalahan pada diri pelaku sebagai dasar untuk membebaskan pertanggungjawaban pidana. hal ini berkaitan dengan prinsip *geen straf zonder schuld* atau tiada pidana tanpa kesalahan, yang menempatkan kesalahan sebagai salah satu dasar penting dalam menentukan dapat atau tidaknya seseorang dipidana. Dalam konteks penyalahgunaan *deepfake*, bentuk kesalahan tersebut terutama berkaitan dengan apakah pelaku dengan sengaja menggunakan teknologi tersebut untuk melakukan suatu perbuatan yang dilarang atau akibat yang timbul terjadi karena kealpaan yang memenuhi ketentuan pidana.

Kesalahan pelaku dalam penyalahgunaan *deepfake* pada dasarnya dapat berbentuk kesengajaan atau kealpaan. Kesengajaan menunjukkan adanya kehendak atau pengetahuan pelaku yang berkaitan dengan perbuatan yang dilakukannya, sedangkan kealpaan berkaitan dengan kurang kehati-hatian dalam melakukan suatu perbuatan sehingga menimbulkan akibat yang dilarang oleh hukum. Perbedaan tersebut penting karena setiap penggunaan teknologi *deepfake* secara otomatis menunjukkan adanya kesalahan pidana. harus dilihat hubungan antara keadaan batin pelaku, tindakan menggunakan teknologi tersebut, dan akibat yang ditimbulkan. Dengan demikian, penilaian terhadap kesalahan tidak hanya melihat keberadaan konten *deepfake*, tetapi juga proses dan keadaan yang melatarbelakangi pembuatannya serta penggunaannya oleh pelaku.²⁰

Dalam penyalahgunaan *deepfake*, kesengajaan dapat terlihat ketika pelaku secara sadar memilih untuk menggunakan teknologi tersebut sebagai sarana melakukan perbuatan yang merugikan pihak lain. Misalnya, pelaku secara sadar mengambil foto atau suara seseorang, memanipulasinya menggunakan teknologi kecerdasan buatan, kemudian menyebarkan hasil manipulasi tersebut untuk menipu, merusak nama baik, memeras, atau melakukan perbuatan lain yang dilarang. Rangkaian tindakan tersebut menunjukkan adanya hubungan antara kehendak pelaku dengan penggunaan teknologi *deepfake*. Hal ini juga menunjukkan bahwa penyalahgunaan teknologi tersebut pada dasarnya dapat digunakan sebagai sarana untuk melakukan tindak pidana yang telah dikenal sebelumnya, sehingga aspek kesalahan pelaku tetap menjadi bagian penting dalam menentukan pertanggungjawaban pidananya.

Kesengajaan dalam penyalahgunaan *deepfake* juga dapat dilihat dari adanya pengetahuan pelaku terhadap karakteristik teknologi yang digunakan. Apabila seseorang mengetahui bahwa konten yang dibuat merupakan hasil manipulasi dan tetap menggunakan atau menyebarkannya untuk menciptakan kesan seolah-olah konten tersebut benar, maka keadaan tersebut dapat menjadi dasar untuk menilai adanya kesengajaan. Hal ini semakin terlihat apabila pelaku melakukan serangkaian tindakan yang terencana, seperti memilih korban, mengumpulkan bahan berupa foto atau suara korban, melakukan manipulasi, menentukan isi konten, kemudian menyebarkannya kepada pihak lain. Rangkaian tersebut menunjukkan bahwa penggunaan *deepfake* bukan sekedar tindakan teknis, melainkan dapat menjadi bagian dari kehendak pelaku dalam mencapai tujuan tertentu.

Sementara itu, kealpaan mempunyai karakteristik yang berbeda dengan kesengajaan. Kealpaan pada prinsipnya berkaitan dengan keadaan ketika seseorang tidak menghendaki terjadinya akibat yang dilarang, tetapi akibat tersebut timbul karena kurangnya kehati-hatian atau perhatian yang seharusnya dilakukan. Namun, dalam konteks hukum pidana Indonesia, kealpaan tidak dapat secara otomatis digunakan untuk membebaskan pertanggungjawaban pidana dalam setiap penyalahgunaan *deepfake*. Penerapan bentuk kesalahan berupa kealpaan harus terlebih dahulu melihat ketentuan pidana yang menjadi dasar pemidanaan terhadap perbuatan *deepfake* yang dilakukan.

Ketentuan tersebut mempunyai arti penting dalam menentukan pertanggungjawaban pidana terhadap penyalahgunaan *deepfake*. Tidak setiap akibat yang muncul dari penggunaan teknologi dapat langsung dibebankan kepada seseorang sebagai tindak pidana karena kealpaan. Harus terdapat dasar hukum yang secara tegas memungkinkan pemidanaan karena kealpaan dan harus dapat dibuktikan pula adanya hubungan antara kelalaian pelaku dengan akibat yang ditimbulkan. Sebaliknya, apabila pelaku dengan sadar menggunakan *deepfake* untuk menghasilkan representasi palsu dan kemudian

²⁰Rocky Marbun dan Maisha Ariani, "Melacak Mens Rea Dalam Penyebaran Berita Bohong Melalui Whatsapp Group: Mengenal Sekilat Psikolinguistik Dalam Hukum Pidana", *Jurnal Hukum Pidana Dan Kriminologi*, Volume 3, Nomor 2, (2022): 72.

menggunakannya untuk melakukan tindak pidana, maka bentuk kesalahan yang lebih relevan untuk dianalisis adalah kesengajaan. Dengan demikian, penentuan bentuk kesalahan harus dilakukan berdasarkan fakta konkret mengenai tindakan pelaku, pengetahuan pelaku terhadap perbuatannya, tujuan penggunaan *deepfake*, serta akibat yang ditimbulkan.

Terlihat dari bahasan diatas bahwa dalam perspektif hukum pidana Indonesia, persoalan utamanya bukan semata-mata mengenai keberadaan teknologi *deepfake*, melainkan mengenai bagaimana perbuatan yang dilakukan melalui teknologi tersebut dapat dipertanggung jawabkan secara pidana. sampai saat ini, belum terdapat ketentuan perundang-undangan yang secara khusus menyebut *deepfake* sebagai suatu jenis tindak pidana tersendiri. Dengan demikian, penyalahgunaan *deepfake* masih harus didiskualifikasikan berdasarkan tindak pidana yang dilakukan melalui teknologi tersebut dan ketentuan pidana yang relevan. Hal ini menunjukkan bahwa perkembangan teknologi telah bergerak lebih cepat dibandingkan dengan pembentukan norma pidana yang secara spesifik mengaturnya.

Ketiadaan rumusan khusus mengenai *deepfake* bukan berarti pelaku selalu terbebas dari pertanggungjawaban pidana. UU No. 1 Tahun 2023 tentang KUHP, telah menjadi dasar umum hukum pidana nasional. Akan tetapi di dalam KUHP saat ini tidak merumuskan *deepfake* sebagai delik tersendiri. Oleh karena itu, pertanggungjawaban pidana terhadap pelaku tetap dapat dilakukan dengan mengidentifikasi perbuatan konkret yang dilakukan menggunakan teknologi tersebut. seperti apabila *deepfake* digunakan untuk memperoleh keuntungan secara melawan hukum melalui tipu muslihat, maka perbuatan tersebut dapat dianalisis berdasarkan ketentuan mengenai penipuan; apabila digunakan untuk menyerang kehormatan seseorang, maka dapat dianalisis berdasarkan ketentuan mengenai penghinaan atau pencemaran nama baik; sedangkan penggunaan *deepfake* untuk mengancam seseorang dapat dikaitkan dengan ketentuan pidana mengenai pemerasan atau pengancaman sesuai dengan fakta perkaranya.

Persoalan tersebut menunjukkan adanya keterbatasan pengaturan yang bersifat spesifik terhadap modul *deepfake*. Peraturan yang ada pada dasarnya mengatur perbuatan pidana dan bukan secara khusus teknologi yang digunakan untuk melakukan perbuatan tersebut. pendekatan demikian memang memungkinkan hukum pidana tetap diterapkan terhadap pelaku, tetapi dapat menimbulkan persoalan ketika karakteristik *deepfake* tidak sepenuhnya sesuai dengan unsur tindak pidana konvensional. Sebagai contoh, dalam penyalahgunaan identitas melalui manipulasi wajah atau suara, persoalan hukumnya tidak hanya terletak pada tindakan membuat konten palsu, tetapi juga pada proses memperoleh bahan digital, memanipulasi identitas, menciptakan representasi palsu, dan menyebarkanluaskannya kepada pihak lain. Oleh sebab itu, ketiadaan rumusan khusus dapat menimbulkan perbedaan penafsiran mengenai ketentuan pidana yang paling tepat digunakan serta berpotensi menciptakan ketidakpastian dalam proses penegakan hukum.

Atas kondisi tersebut, perlu adanya penyempurnaan aturan yang secara lebih khusus mengatur penyalahgunaan teknologi kecerdasan buatan. Pengaturan tersebut tidak harus selalu menjadikan setiap penggunaan *deepfake* sebagai tindak pidana, karena teknologi tersebut juga dapat digunakan untuk kepentingan yang sah. Yang lebih penting adalah merumuskan secara jelas batas antara penggunaan yang sah dengan penyalahgunaan yang merugikan atau membahayakan kepentingan hukum seseorang. Sehingga dengan adanya pembaharuan hukum pidana terhadap penyalahgunaan teknologi *deepfake* dapat memastikan perkembangan teknologi tetap berada dalam batas hukum dan bahwa pelaku yang memenuhi unsur pertanggungjawaban pidana dapat dimintai pertanggungjawaban secara jelas dan mendapatkan sanksi pidana yang proporsional.

Pengenaan sanksi pidana terhadap pelaku penyalahgunaan teknologi *deepfake* merupakan tahap lanjutan setelah dapat dibuktikan adanya tindak pidana, kemampuan bertanggung jawab, serta kesalahan pada diri pelaku. Sanksi pidana tidak dapat dijatuhkan semata-mata karena seseorang menggunakan teknologi *deepfake*, melainkan harus didasarkan pada perbuatan konkret yang memenuhi unsur tindak pidana dan dapat dipertanggungjawabkan kepada pelakunya. Dalam konteks hukum pidana Indonesia, *deepfake* belum dirumuskan sebagai suatu jenis tindak pidana tersendiri, sehingga penerapan sanksinya dilakukan dengan menggunakan ketentuan pidana yang sesuai dengan bentuk penyalahgunaan dan akibat yang ditimbulkan. Kondisi tersebut menunjukkan bahwa hubungan antara

perbuatan menggunakan *deepfake* dan sanksi pidana harus terlebih dahulu dibangun melalui pembuktian unsur tindak pidana yang dilakukan oleh pelaku.²¹

Salah satu ketentuan yang memiliki keterkaitan paling langsung dengan penggunaan *deepfake* adalah Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 yang menyatakan bahwa; “setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik”. Ketentuan ini relevan dengan karakteristik *deepfake* karena teknologi tersebut pada dasarnya menghasilkan atau memanipulasi konten digital sehingga suatu representasi palsu dapat tampak sebagai keadaan yang benar. Dengan demikian, apabila perbuatan *deepfake* memenuhi unsur pasal 35, ketentuan tersebut dapat menjadi salah satu dasar untuk membebankan pertanggungjawaban pidana kepada pelaku.²²

Terhadap pelanggaran pasal 35 tersebut, Pasal 51 ayat (1) UU ITE menentukan ancaman pidana berupa; “setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah)”. Ancaman tersebut menunjukkan bahwa hukum Indonesia telah menyediakan instrumen pemidanaan terhadap perbuatan manipulasi informasi elektronik yang bertujuan menghasilkan data seolah-olah autentik, meskipun istilah *deepfake* sendiri belum disebut secara eksplisit dalam rumusan delik. Oleh karena itu, dalam perkara penyalahgunaan *deepfake*, penerapan Pasal 35 jo Pasal 51 ayat (1) tidak dapat dilakukan hanya berdasarkan fakta bahwa konten tersebut merupakan *deepfake*, tetapi harus dibuktikan pula adanya unsur kesengajaan, sifat tanpa hak atau melawan hukum, tindakan manipulasi atau penciptaan informasi elektronik, serta tujuan agar informasi tersebut dianggap sebagai data autentik.²³

Selain ketentuan mengenai manipulasi informasi elektronik, sanksi terhadap pelaku juga dapat mengikuti tindak pidana yang menjadi tujuan atau akibat penggunaan *deepfake*. Artinya, apabila dilakukan untuk melakukan penipuan, pencemaran nama baik, pemerasan, atau penyebaran konten yang melanggar kesusilaan, maka ketentuan pidana yang mengatur perbuatan tersebut dapat diterapkan sepanjang seluruh unsur deliknya dipenuhi. Pendekatan demikian penting karena *deepfake* pada dasarnya merupakan sarana atau modus yang digunakan untuk melakukan tindak pidana. Dengan demikian, jenis dan beratnya sanksi tidak semata-mata ditentukan oleh teknologi yang digunakan, tetapi juga oleh karakter perbuatan pidana yang terbukti dilakukan oleh pelaku.

Penerapan sanksi tersebut juga harus mempertimbangkan tingkan kesalahan dan akibat yang ditimbulkan oleh perbuatan pelaku. Dalam penyalahgunaan *deepfake*, tingkat kesalahan dapat terlihat dari cara pelaku memperoleh bahan, melakukan manipulasi, menggunakan hasil manipulasi, serta menyebarkannya kepada pihak lain. Semakin jelas tujuan kriminal dan semakin besar akibat yang ditimbulkan, hal ini penting untuk menentukan pertanggungjawaban pidana dari tindakan tersebut. hal ini menunjukkan bahwa sanksi pidana tidak boleh dipandang terpisah dari unsur kesalahan yang telah dibahas sebelumnya.

Selain itu, dalam perkara tertentu satu tindakan *deepfake* juga dapat menimbulkan lebih dari satu kepentingan hukum yang dilanggar, misalnya ketika suatu konten hasil manipulasi sekaligus menyerang identitas, kehormatan, dan privasi korban. Keadaan tersebut perlu dianalisis berdasarkan perbuatan konkret yang dilakuakn dan ketentuan pidana yang memenuhi unsur, sehingga sanksi yang dijatuhkan tetap berlandaskan asas legalitas dan tidak semata-mata didasarkan pada beratnya dampak yang ditimbulkan. Oleh karena itu, meskipun *deepfake* memiliki karakteristik teknologi yang baru, pemidanaan terhadap pelakunya tetap harus mengikuti prinsip bahwa tidak ada pidana tanpa ketentuan pidana yang telah ada sebelumnya serta tidak ada pertanggungjawaban pidana tanpa kesalahan. Dalam hal *deepfake* digunakan untuk konten pornografi non konsensual, misalnya penelitian hukum nasional

²¹Supuan Sultan Al-Alif dan Cik Marhayati, *Op.Cit.*, hlm. 1172.

²²*Ibid.*

²³*Ibid.*, hlm, 1173.

menunjukkan bahwa ketentuan dalam UU ITE, UU Pornografi, dan UU Perlindungan Data Pribadi dapat menjadi dasar hukum sesuai dengan perbuatan dan unsur yang terbukti.²⁴

Berdasarkan uraian mengenai pertanggungjawaban pidana terhadap teknologi *deepfake*, dapat dipahami bahwa pertanggungjawaban pidana tetap dapat dibebankan kepada pelaku sepanjang terpenuhinya unsur kemampuan bertanggung jawab, kesalahan, dan perbuatan pidana yang menjadi dasar pemidanaan. Penyalahgunaan *deepfake* tidak dapat dipandang hanya sebagai persoalan penggunaan teknologi, tetapi harus dilihat dari perbuatan konkret yang dilakukan oleh pelaku, tujuan penggunaan teknologi tersebut, serta akibat yang ditimbulkan. Meskipun *deepfake* belum dirumuskan sebagai tindak pidana khusus dalam peraturan perundang-undangan Indonesia, penggunaan teknologi tersebut sebagai sarana untuk melakukan penipuan, pencemaran nama baik, pemerasan, penyalahgunaan identitas, maupun perbuatan pidana lainnya tetap dapat dikenakan ketentuan pidana yang relevan sepanjang unsur-unsurnya terpenuhi. Dengan demikian, perkembangan teknologi tidak menghilangkan prinsip pertanggungjawaban pidana terhadap manusia sebagai pihak yang mengendalikan dan menyalahgunakan teknologi tersebut.

Pada akhirnya, pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* menunjukkan perlunya penerapan hukum pidana yang tetap berpegang pada asas legalitas dan asas kesalahan, sekaligus mampu merespons perkembangan bentuk kejahatan digital. Penentuan pertanggungjawaban harus dilakukan secara cermat dengan mempertimbangkan kemampuan bertanggung jawab pelaku, bentuk kesalahan yang dilakukan, hubungan antara perbuatan dan akibat, serta ketentuan pidana yang dapat diterapkan terhadap perbuatan tersebut. Kondisi belum adanya pengaturan khusus mengenai *deepfake* juga menunjukkan adanya kebutuhan untuk memperkuat dan mengembangkan kebijakan hukum pidana agar mampu memberikan kepastian hukum serta perlindungan yang lebih optimal terhadap korban. Oleh karena itu, pertanggungjawaban pidana terhadap penyalahgunaan teknologi *deepfake* merupakan bagian penting dalam upaya memastikan bahwa kemajuan teknologi digital tidak berkembang menjadi sarana kejahatan yang berada di luar jangkauan hukum pidana.

SIMPULAN

Berdasarkan penjelasan dari hasil pembahasan sebagai jawaban dari permasalahan yang ditimbulkan dalam pendahuluan diatas, maka penulis menyimpulkan sebagai berikut:

1. Penyalahgunaan teknologi *deepfake* dapat menjadi sarana dalam melakukan berbagai bentuk tindak pidana digital karena kemampuan memanipulasi wajah, suara, maupun identitas seseorang sehingga menghasilkan informasi atau konten yang tampak seolah-olah benar. Pemanfaatan teknologi tersebut secara melawan hukum dapat digunakan untuk melakukan penipuan, pencemaran nama baik, pemerasan, penyebaran konten yang melanggar kesusilaan, serta perbuatan digital lainnya yang menimbulkan kerugian bagi korban. Oleh karena itu, keberadaan *deepfake* tidak hanya menimbulkan persoalan teknologi, tetapi juga persoalan hukum, khususnya ketika teknologi tersebut digunakan dengan tujuan melakukan perbuatan yang memenuhi unsur suatu tindak pidana.
2. Pertanggungjawaban pidana terhadap pelaku penyalahgunaan *deepfake* tetap dapat diterapkan meskipun belum terdapat ketentuan pidana yang secara khusus menggunakan istilah *deepfake*. Pertanggungjawaban dapat dikenakan dengan mengaitkan perbuatan pelaku pada ketentuan pidana yang relevan sesuai dengan bentuk tindak pidana yang dilakukan, sepanjang terpenuhinya unsur tindak pidana, adanya kesalahan, serta tidak terdapat alasan yang menghapuskan pertanggungjawaban pidana. Dengan demikian, perkembangan teknologi *deepfake* tidak menghilangkan pertanggungjawaban hukum atas perbuatan yang dilakukan melalui teknologi tersebut, melainkan menuntut penerapan hukum secara tepat agar mampu memberikan kepastian hukum, perlindungan terhadap korban, dan penanggulangan terhadap perkembangan kejahatan digital di Indonesia.

²⁴Faudi Isnawan, "Deepfake Pornography: How Criminal Liability Of Perpetrators In The Indonesia Criminal Law Framework", *Jurnal Magister Hukum Udayana*, Volume 13, Nomor 3, (2024): 7246.

DAFTAR PUSTAKA

Buku

- Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana, 2017.
- Chazawi, Adami. *Pelajaran Hukum Pidana Bagian I*. Jakarta: Rajawali Pers, 2005.
- Nasution, Bahder Johan. *Metode Penelitian Ilmu Hukum*. Bandung: Mandar Maju, 2008.
- Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajagrafindo Persada, 2012.
- Widodo. *Hukum Pidana di Bidang Teknologi (Cybercrime Law): Telaah Teoritik dan Bedah Kasus*. Yogyakarta: Aswaja Pressindo, 2013.

Peraturan Perundang-Undangan

- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana
- Undang-Undang Nomor 11 Tahun 2008 yang di ubah menjadi Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Jurnal

- Al-Alif, Sultan, Supuan, dan Cik Marhayati. "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake Di Indonesia". *Legal Standing: Jurnal Ilmu Hukum* 9, no. 5 (2025): 1165-1175.
- Alyani, Aisyah. 2024. "Dampak Penyalahgunaan Deepfake Dalam Memanipulasi Visual: Menguk Potensi Infopocalypse Di Era Post Truth Terhadap Asumsi Masyarakat Pada Media Massa". *Jurnal Kawistara* 14 (3): 408.
- Faqih, Muhammad, dan E.S. Priowirjanto. 2022. "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia". *Jurnal Indonesia Sosial Teknologi* 3 (11): 1158.
- Gresmelian, Asri, dan Wiwik Afifah. 2024. "Criminal Responsibility Of Artificial Intelligence Committing Deepfake Crimes In Indonesia". *Asian Journal Of Social And Humanities* 2 (4): 777.
- Isnawan, Faudi. 2024. "Deepfake Pornography: How Criminal Liability Of Perpetrators In The Indonesia Criminal Law Framework". *Jurnal Magister Hukum Udayana* 13 (3): 7246.
- Lukman Ibrahim, Aji. 2024. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Perlindungan Negara". *Jurnal USM Law Review* 7 (2): 604.
- Marbun, Rocky, dan Maisha Ariani. 2022. "Melacak Mens Rea Dalam Penyebaran Berita Bohong Melalui Whatsapp Group: Mengenal Sekilat Psikolinguistik Dalam Hukum Pidana". *Jurnal Hukum Pidana Dan Kriminologi* 3 (2): 72.
- Martina Putri, Ni Putu, M.S. Hartono, dan I Dewa Gede H.Y. "Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake Dalam Tindak Pidana Pencemaran Nama Baik Berbasis Artificial Intelligence". *Jurnal Pacta Sunt Servanda* 5, no. 2 (2024): 123.
- Muhammad Hapid, Fasa Ija S., dan M. Yayan. "Penerapan Asas Green Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake". *Jurnal USM Law Review* 7, no. 3 (2024): 1156.
- Noerman, Chiquita Thefirstly. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Perlindungan Negara". *Jurnal USM Law Review* 7, no. 2 (2024): 610.
- Putra, Rio Irandha. "Deepfake Sebagai Sarana Pemerasan Dalam Perspektif Hukum Pidana Indonesia". *Risalah Hukum* 22, no. 1 (2026): 26.
- Sandoval, Maria-Paz. 2024. "Threat Of Deepfake To The Criminal Justice System: A Systematic Review". *Crime Science* 13 (41): 20.
- Syafiq, Muhammad. "Artificial Intelligence-Based Deepfake Crimes: A Conception Of Culpability Principle As A Criminal Liability Reform". *Reformasi Hukum* 29, no. 2 (2025): 55-65.
- U.S, Sarah Amanda, dan Diana Lukitasari. "Konten Gambar Dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik". *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 13, no. 2 (2024): 165-175.
- Wiraguna, Sidi [Ahya Wiraguna]. 2024. "Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia". *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum* 3 (3): 59.