TINDAK PIDANA PEMALSUAN WAJAH YANG MENGGUNAKAN TEKNOLOGI *ARTIFICIAL INTELLIGENCE* (AI) MENURUT PERATURAN PERUNDANG-UNDANGAN [1]

Oleh :
Stevi Claudia Logor [2]
Herlyanty Y. A. Bawole [3]
Herry F. D. Tuwaidan [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan hukum terhadap pelaku pemalsuan wajah yang menggunakan teknologi (AI) di Indonesia dan untuk mengetahui mekanisme perlindungan hukum bagi korban pemalsuan wajah yang menggunakan teknologi AI di Indonesia sesuai dengan sistem hukum yang berlaku. Dengan menggunakan metode penelitian hukum normatif, dapat ditarik kesimpulan 1. Ketentuan dalam kitab undang-undang hukum pidana (KUHP) dapat digunakan untuk menjerat perbuatan yang mengandung unsur penipuan, pencemaran nama baik, maupun penyebaran berita bohong. UU ITE memberikan pengaturan yang lebih spesifik terkait perbuatan yang dilakukan melalui media elektronik, termasuk penyebaran konten yang melanggar hukum, seperti penghinaan, pelanggaran kesusilaan, dan penyebaran informasi yang merugikan masyarakat. Sementara itu, UU PDP juga memiliki relevansi yang signifikan, mengingat penggunaan data biometrik seperti wajah dan suara dalam teknologi *deepfake* merupakan bagian dari data pribadi yang harus dilindungi dan tidak dapat diproses tanpa persetujuan dari subjek data. 2. Perlindungan hukum terhadap korban pemalsuan wajah melalui teknologi kecerdasan buatan (AI) berbasis *deepfake* di Indonesia pada tahap ini masih bersifat fragmentaris dan normatif umum, mengandalkan kerangka regulasi yang ada seperti Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru), serta Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban.

Kata Kunci : ***pemalsuan wajah, AI***

PENDAHULUAN

A. Latar Belakang

Teknologi kecerdasan buatan (AI) adalah suatu bidang dalam ilmu komputer yang berfokus pada pembuatan sistem atau mesin yang dapat meniru kecerdasan manusia, seperti kemampuan untuk berpikir, belajar, mengenali pola, memahami bahasa, dan mengambil keputusan secara mandiri. Menurut H. A. Simon, kecerdasan buatan (AI) merupakan studi penelitian, aplikasi dan instruksi yang berkaitan erat dengan pemrograman komputer untuk melakukan suatu hal yang dalam pandangan manusia dinilai cerdas.[5]

Deepfake berasal dari dua kata: deep learning (pembelajaran mendalam) dan fake (palsu). *Deepfake* adalah hasil manipulasi video, gambar, atau suara menggunakan algoritma AI sehingga menyerupai orang lain secara sangat realistis.[6] Menurut Chesney & Citron, *deepfake* merupakan "konten sintetis yang dihasilkan oleh algoritma AI yang mampu meniru penampilan dan suara seseorang secara meyakinkan". [7] Dalam konteks hukum, *deepfake* dikategorikan sebagai bentuk manipulasi digital yang berpotensi melanggar hak privasi, reputasi, serta hukum pidana jika digunakan untuk tujuan jahat. Bentuk penyalahgunaan teknologi *deepfake* antara lain:

1. Pemalsuan identitas, membuat video palsu dengan wajah seseorang untuk penipuan.
2. Pencemaran nama baik, menyebarkan konten yang meniru wajah tokoh publik untuk menjatuhkan reputasi.
3. Pornografi nonconsensual, mengganti wajah orang dalam video porno tanpa persetujuan.
4. Manipulasi politik dan disinformasi, membuat video palsu tokoh politik guna memengaruhi opini public

Deepfake merupakan media audio visual yang tidak asli dan dibuat dengan kecerdasan buatan, tidak berarti bahwa keaslian *deepfake* dapat dengan mudah dikenali secara langsung. Sebaliknya, *deepfake* bisa tampak sangat realistis dan otentik tergantung pada seberapa banyak data yang digunakan. Istilah *Deepfake* muncul pada 2017 oleh pengguna reddit yang merupakan seorang anonym untuk teknologi yang

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010363
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Kaharuddin dan Zul Amirul Haq, 2024, *Kecerdasan Buatan Aspek Perlindungan Hukum Di Era Globalisasi*, Kencana, hlm. 10.
[6] Kietzmann & Jill Angell, *Deepfakes: Trick or Treat? Understanding the Implications of Synthetic Media, Business Horizons* 63, no. 2 (2020): 135–146.
[7] Chesney, R., & Citron, D. K., 2019. *Deep fakes: A Looming Challenge For Privacy, Democracy, And National Security*. California Law Review, 107(6), 1753–1819.

menggunakan Deeplearning untuk melatih program komputer dalam mengumpulkan data video seseorang. Program ini selanjutnya melakukan peniruan ekspresi wajah dan Gerakan hingga menjadikannya video palsu. [8] Semakin banyak sampel suara dan gambar wajah dari individu yang wajah dan/atau suaranya dimasukkan dalam *deepfake* yang digunakan, maka *deepfake* yang dihasilkan akan semakin baik dan nyata. Namun dalam *deepfake* tersebut ada beberapa wajah atau visual yang digunakan mirip dengan suara aslinya tanpa adanya perbedaan sedikitpun.

Dampak hukum dan sosial dari penyalahgunaan *deepfake* sangat besar yaitu hilangnya kepercayaan masyarakat terhadap informasi digital, kerugian material korban, serta pelanggaran hak moral dan hak privasi. Dalam konteks hukum, AI menimbulkan persoalan baru karena kemampuannya untuk bertindak secara otonom dan menghasilkan output yang sulit dilacak sumbernya. Salah satu bentuk penerapan AI yang paling kontroversial adalah *deepfake*, yaitu teknologi yang mampu memanipulasi wajah atau suara seseorang secara realistis sehingga tampak asli.

Perkembangan AI memberikan manfaat besar di bidang industri kreatif, pendidikan, hingga keamanan, penggunaan teknologi ini juga berpotensi menimbulkan permasalahan hukum dan etika. Salah satu permasalahan yang muncul adalah tindakan pemalsuan wajah menggunakan teknologi AI untuk tujuan-tujuan yang melanggar hukum, seperti pencemaran nama baik, penipuan digital, penyebaran konten pornografi nonkonsensual, maupun tindak pidana lain yang melanggar hak privasi seseorang. AI dapat bekerja secara otomatis, sehingga sering kali sulit menentukan siapa pelaku utama yang harus dimintai pertanggungjawaban.

Salah satu bentuk penerapan teknologi AI yang kini banyak diperbincangkan adalah teknologi *deepfake*. Suatu metode yang memanfaatkan algoritma pembelajaran mesin untuk memanipulasi atau memalsukan wajah seseorang secara sangat realistis. Teknologi ini mampu menghasilkan video, gambar, atau suara yang menyerupai individu tertentu, sehingga sulit dibedakan antara hasil manipulasi dengan yang asli.

Dalam sistem hukum di Indonesia belum secara tegas mengatur mengenai penggunaan teknologi kecerdasan buatan dalam kasus pemalsuan wajah atau manipulasi identitas digital. Namun, beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dapat dijadikan dasar hukum untuk menjerat pelaku pemalsuan wajah digital tersebut.[9]

Ketiadaan pengaturan khusus mengenai penggunaan AI dan pemalsuan wajah menimbulkan tantangan dalam penegakan hukum. Di satu sisi, teknologi AI terus berkembang pesat dan sulit dibendung; di sisi lain, aparat penegak hukum menghadapi kesulitan dalam menilai sejauh mana pertanggungjawaban pidana dapat dikenakan kepada pelaku yang menggunakan teknologi ini. Pemalsuan wajah berbasis Artificial Intelligence (AI) atau *deepfake* merupakan bentuk manipulasi digital yang menggunakan algoritma *machine learning* untuk menciptakan citra atau video yang meniru wajah seseorang dengan sangat realistis. Dalam konteks hukum Indonesia, tindakan tersebut dapat dikategorikan sebagai pelanggaran terhadap kehormatan, reputasi, dan data pribadi seseorang, serta dapat menimbulkan kerugian baik secara moral maupun materiil.

Penyalahgunaan teknologi *deepfake* telah berdampak luas di berbagai bidang, terutama dalam aspek privasi, keamanan digital, serta kepercayaan publik terhadap informasi yang beredar di ruang digital dan media sosial. Teknologi ini memungkinkan manipulasi wajah, suara, dan konten digital dengan tingkat realisme tinggi sehingga dapat menciptakan video hoaks yang tampak autentik padahal palsu, yang pada gilirannya berpotensi menyesatkan opini publik dan merusak kepercayaan terhadap lembaga, tokoh, maupun media massa.

Deepfake dapat muncul dalam berbagai bentuk teknologi yang menjadi tantangan serius dalam mengetahui keaslian pada konten multimedia. *Deep Learning*, yang pada awalnya dikembangkan untuk kepentingan industry seperti pengenalan wajah dan suara, kini juga dimanfaatkan dalam pembuatan konten palsu berbasis teknologi *deepfake*[10].

Beberapa kasus yang telah terjadi di Indonesia menunjukkan bahwa teknologi ini

[8] Situmeang, B. S., dkk., 2024. *Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deepfake Pada Selebritas di Twitter*. Device, 14(1). Hlm. 81

[9] Kitab Undang-Undang Hukum Pidana (KUHP); UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE).; UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

[10] Anfa'un Nisa'.F.R., Syariffudin., et al., 2025, *Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik Deepfake*, Perspektif Administrasi Publik dan Hukum, Vol. 2, No. 1, hlm. 250.

sering digunakan untuk membuat video hoaks yang menyesatkan opini publik, serta dalam modus penipuan daring.

Contoh kasus yang spesifik tentang pemalsuan wajah menggunakan AI di Indonesia menurut laporan aparat Bareskrim Polri (Direktorat Tindak Pidana Siber) mengungkap kasus di mana pelaku menggunakan wajah Prabowo Subianto yang diedit dengan teknologi *deepfake* untuk melakukan modus penipuan. Modusnya video palsu yang menampilkan pejabat negara (seolah-seorang pejabat mengumumkan bantuan atau program) kemudian dikirim atau diunggah ke media sosial, korban diarahkan menghubungi nomor WhatsApp yang dicantumkan dan diminta mentransfer uang dengan alasan administrasi pencairan bantuan. Dalam analisis forensik, penggunaan software untuk mendeteksi *deepfake* menghasilkan skor tinggi (skor "1.00" untuk GAN) yang menunjukkan konten tersebut adalah hasil manipulasi penuh.[11]

Pelaku pemalsuan wajah dengan AI dapat dikenai pertanggungjawaban pidana jika memenuhi unsur kesengajaan (dolus) pelaku dengan sadar membuat konten manipulatif menggunakan AI, unsur perbuatan melawan hukum dalam penggunaan wajah orang lain tanpa izin, dan unsur akibat hukum yang menimbulkan kerugian, baik secara materiil maupun immateriil bagi korban. Jika ketiga unsur ini terpenuhi, pelaku dapat dijerat dengan gabungan pasal-pasal dari UU ITE, KUHP, dan UU PDP. [12]

B. Perumusan Masalah

1. Bagaimana pengaturan hukum terhadap pelaku pemalsuan wajah yang menggunakan teknologi (AI) di Indonesia?
2. Bagaimana mekanisme perlindungan hukum bagi korban pemalsuan wajah yang menggunakan teknologi AI di Indonesia sesuai dengan sistem hukum yang berlaku?

C. Metode Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif (yuridis normatif).

PEMBAHASAN

A. Pengaturan Hukum Terhadap Pelaku Pemalsuan Wajah yang Menggunakan Teknologi (AI) di Indonesia

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah membawa dampak signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam bidang hukum. Salah satu bentuk perkembangan tersebut adalah munculnya teknologi *artificial intelligence* (AI) yang mampu menciptakan manipulasi konten digital secara canggih, termasuk pemalsuan wajah atau yang dikenal dengan istilah *deepfake*. Teknologi ini memungkinkan seseorang untuk mengubah atau merekayasa wajah individu lain dalam suatu media digital sehingga tampak seolah-olah asli, padahal kenyataannya merupakan hasil rekayasa. Fenomena pemalsuan wajah berbasis teknologi AI menimbulkan berbagai permasalahan hukum, terutama ketika teknologi tersebut disalahgunakan untuk tujuan yang melanggar hukum, seperti penipuan, pencemaran nama baik, hingga pelanggaran privasi.

AI memiliki kemampuan untuk menganalisis dan menalar data besar secara rasional untuk tujuan mengambil keputusan secara mandiri guna mencapai tujuan tertentu. Selain itu, kecerdasan yang dimiliki AI memungkinkannya untuk memberikan jawaban atas pertanyaan, melaksanakan perintah, serta melakukan berbagai tindakan yang menyerupai perilaku manusia. walaupun AI mampu membangun pola pikir yang menyerupai kemampuan kognitif manusia, hal tersebut tidak dapat dijadikan dasar untuk menganggap bahwa AI adalah manusia. seiring berjalannya waktu, AI dapat memberikan ancaman yang lebih besar ketika terdapat pihak yang menggunakan varian baru AI yang berpotensi melanggar etika. Keberadaan AI yang bebas dapat digunakan untuk membuat disinformasi yang lebih meyakinkan, memproduksi lebih banyak konten palsu secara masif, bahkan dapat mengubahnya menjadi alat yang memindai sosial media yang menjurus kepada provokatif. Teknologi yang dapat digunakan untuk membuat sekaligus memanipulasi konten berbentuk gambar, suara, dan video yang realistik disebut sebagai *Deepfake*. Konsep *Deepfake* dipahami sebagai gabungan dari teknologi deeplearning dan (AI), di mana gambar dan suara palsu dikompilasi, lalu digabungkan melalui algoritma pembelajaran mesin untuk menghasilkan representasi orang atau peristiwa yang sebenarnya tidak pernah ada atau tidak terjadi. Perubahan besar dalam kehidupan manusia secara nyata telah dihasilkan oleh pesatnya perkembangan teknologi, yang membawa konsekuensi tak terelakkan. [13] Oleh

[11] Kompas.com., *Bareskrim usut kemungkinan sindikat penipuan video "deepfake" Prabowo*, 7 Februari 2025.
[12] *Ibid*, hlm. 9.
[13] Martinelli, I., Dkk. 2023. *Urgensi Pengaturan dan Perlindungan Rights of Privacy terhadap Artificial*

karena itu, diperlukan adanya pengaturan hukum yang jelas dan tegas untuk mengatur serta menindak pelaku yang melakukan pemalsuan wajah dengan menggunakan teknologi AI.

Teknik *Deepfake* dengan aplikasi FakeApp digunakan untuk menukar wajah seseorang dengan orang lain. FakeApp atau aplikasi palsu ini merupakan perangkat lunak yang membutuhkan sejumlah data yang besar untuk menghasilkan data yang baik. Data ini akan disalurkan ke sistem untuk memproses model wajah seseorang yang ditargetkan. Penciptaan wajah palsu ini melibatkan ekstraksi gambar dan video yang nantinya menghasilkan gambar atau video palsu yang sempurna. Selanjutnya adalah teknik ekspresi dinamis. Teknik ini merupakan teknik menggunakan waktu dan sistem dengan ketelitian tinggi yang mampu merekonstruksi lebih detail. Generasi *deepfake* selanjutnya adalah teknik pelacakan dengan pendekatan model wajah parametrik.

Pelacakan awal adalah dengan memberi pencahayaan ke sekitar area mulut termasuk ke proksi gigi dan ke dalam mulut. Teknik ini menghasilkan gambar yang detail dan menghasilkan gambar yang lebih dekat. Berdasarkan paparan tersebut tentunya perkembangan teknologi informasi dan kecerdasaan buatan atau AI yang sangat pesat memunculkan sebuah tantangan yang sangat besar. Hal ini karena hampir semua institusi baik pemerintahan, perusahaan, dan masyarakat menggunakan serta bergantung pada sistem informasi digital sehingga rentan terhadap ancaman. Penggunaan teknologi artificial intelligence *deepfake* yang menimbulkan masalah keamanan siber terjadi karena adanya serangan malware, yang mana dapat mempermudah para hacker untuk mengidentifikasi dan menganalisis kelemahan berbagai variasi software secara efisien. Aktivitas para hacker inilah yang kemudian menyebabkan terjadinya tindak pidana siber.

Ada dua metode untuk membuat *deepfake*, pertama yaitu menggunakan algoritma AI bernama encoder. Pertama-tama, kita harus mengumpulkan ribuan foto dari dua orang yang berbeda. Lalu, encoder akan memprosesnya untuk menemukan kemiripan dan memancarkan wajah A ke wajah B di video lain. Selain encoder, *deepfake* juga bisa dibuat menggunakan Generative Adversarial Network atau GAN yang menggunakan komponen generator dan discriminator untuk menghasilkan data sintesis. Secara khusus kejahatan ini belum ada pengaturannya, namun kejahatan seperti ini bisa merujuk kepada ketentuan yang ada di dalam Kitab Undang-undang Hukum Pidana, Undang-undang Perlindungan data pribadi (PDP), Undang-undang Informasi dan Transaksi Elektronik (ITE). [14]Dulu teknologi Deep Fake ini hanya digunakan sebagai wadah hiburan dan lucu-lucuan, baik di sosial media maupun televisi. Namun seiring berjalannya waktu, banyak peluang untuk mendapatkan keuntungan dari teknologi AI ini, maka pelaku penyalahgunaan ini sering kali menggunakan cara ini sebagai cara alternatif untuk menipu orang serta menyebarkan berita atau informasi palsu.

Di Indonesia, penyalahgunaan teknologi kecerdasan buatan (AI) untuk pemalsuan wajah atau *deepfake* belum diatur secara spesifik. Hal ini menimbulkan tantangan bagi penegak hukum dalam menangani kasus *Deepfake* yang semakin marak, seperti penyebaran konten palsu untuk pencemaran nama baik, pemerasan, atau penipuan. Meskipun demikian, terdapat beberapa ketentuan hukum yang relevan dan dapat dijadikan dasar penindakan, yaitu Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).[15] Ketentuan-ketentuan ini memberikan landasan kuat untuk menjerat pelaku, meski interpretasi dan penerapannya memerlukan penyesuaian dengan perkembangan teknologi.

1. Kitab Undang-undang Hukum Pidana
   a. Pasal 263 KUHP
      Pasal ini mengatur perbuatan menyiarkan atau menyebarluaskan berita bohong yang diketahui atau patut diduga kebohongannya, baik melalui media cetak, elektronik, maupun lisan. Relevan untuk kasus *deepfake* yang digunakan menyebarkan hoaks, misalnya video palsu tokoh publik yang memprovokasi konflik sosial atau kerusuhan.
   b. Pasal 433 KUHP

Intelligence dalam Pandangan Hukum sebagai Social Engineering. Jurnal Tana Mana, 4(2), hlm. 157-158.

[14] Adnasohn Aqilla Respati dkk., 2024. *Media Hukum Indonesia (MHI) Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban*, No. 2 : 586, (2024) https://doi.org/10.5281/zenodo.12508126. hlm 587-588.

[15] Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Pasal ini mengatur pencemaran nama baik melalui tulisan atau gambar yang dengan sengaja merendahkan kehormatan atau nama baik seseorang di mata umum. Berlaku untuk *deepfake* berupa video, foto, atau audio palsu yang merusak reputasi, seperti manipulasi wajah korban dalam situasi memalukan atau kriminal.

c. Pasal 492 KUHP
Pasal ini mengatur penipuan yang dilakukan dengan tipu muslihat atau kebohongan sehingga menyebabkan kerugian materiil atau immateriil bagi orang lain. Dapat diterapkan jika *deepfake* dimanfaatkan untuk menipu korban, seperti video palsu untuk pemerasan, penggelapan dana, atau penipuan identitas dalam transaksi online.

2. Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik
   a. Pasal 27 ayat (1) UU ITE
   Pasal ini melarang setiap orang menyebarkan informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan. Relevan untuk *deepfake* berupa video atau gambar palsu bermuatan pornografi non-konsensual (seperti revenge porn), yang merendahkan martabat korban secara digital.
   b. Pasal 27A UU ITE
   Pasal ini melarang penyebaran informasi elektronik dan/atau dokumen elektronik yang berisi penghinaan dan/atau pencemaran nama baik. Berlaku untuk *deepfake* yang memanipulasi wajah seseorang dalam konten memfitnah, seperti video palsu yang menggambarkan korban melakukan tindakan tercela di media sosial.
   c. Pasal 28 ayat (1) UU ITE
   Pasal ini melarang menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Dapat diterapkan pada *deepfake* untuk penipuan online, misalnya video palsu selebriti yang "mengiklankan" produk scam atau memprovokasi kerugian finansial massal.
   d. Pasal 35 UU ITE
   Pasal ini melarang setiap orang dengan sengaja menciptakan atau mengubah informasi elektronik dan/atau dokumen elektronik agar tampak asli atau autentik padahal diketahui tidak asli atau autentik. Secara langsung relevan untuk *deepfake* karena melarang pemalsuan wajah digital atau suara dalam video/audio agar terlihat nyata, seperti dalam pemalsuan pidato atau pernyataan resmi.
   e. Pasal 45A ayat (1) UU ITE
   Pasal ini menetapkan sanksi pidana dan/atau denda paling sedikit Rp1.000.000.000,00 (satu miliar rupiah) bagi pelanggaran Pasal 28 ayat (1). Menekankan konsekuensi berat untuk penyebaran berita bohong *deepfake* yang merugikan konsumen, mendorong penegakan hukum yang tegas di ranah transaksi elektronik.

3. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
   a. Pasal 5 UU PDP
   Pasal ini menetapkan prinsip legalitas, transparansi, dan keadilan dalam pengolahan data pribadi. Relevan untuk *deepfake* karena wajah dan suara termasuk data pribadi biometrik; pengolahan tanpa dasar hukum yang sah melanggar prinsip ini, memastikan akuntabilitas penggunaan AI dalam manipulasi data.
   b. Pasal 17 ayat (1) UU PDP
   Pasal ini melarang pemrosesan data pribadi sensitif (termasuk biometrik seperti wajah) tanpa persetujuan eksplisit dari subjek data. *Deepfake* yang memanfaatkan data wajah tanpa izin jelas melanggar, karena melibatkan pengumpulan, pengolahan, dan distribusi data sensitif tanpa hak.
   c. Pasal 35 UU PDP
   Pasal ini memberikan hak bagi subjek data untuk menuntut ganti rugi materiil maupun immateriil akibat pelanggaran pengolahan data pribadi. Korban *deepfake* dapat menggugat pelaku atas kerugian reputasi, psikologis, atau finansial yang ditimbulkan oleh konten palsu yang menggunakan data pribadinya.
   d. Pasal 47 UU PDP
   Pasal ini menetapkan sanksi pidana bagi pelanggaran tertentu terhadap pengolahan data pribadi, termasuk yang disengaja. Berlaku untuk pembuat atau penyebar *deepfake* yang melanggar privasi data, dengan penekanan pada perlindungan hak dasar individu dari penyalahgunaan teknologi AI.

Berdasarkan uraian pasal-pasal di atas, dapat dipahami bahwa meskipun belum terdapat pengaturan khusus mengenai pemalsuan wajah

berbasis Artificial Intelligence (AI) di Indonesia, berbagai ketentuan dalam peraturan perundang-undangan yang ada, seperti KUHP, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi telah memberikan dasar hukum yang cukup untuk menjerat pelaku penyalahgunaan teknologi tersebut. Namun demikian, kompleksitas dan perkembangan pesat teknologi *Deepfake* menuntut adanysa peraturan yang lebih spesifik dan komprehensif guna memberikan kepastian hokum serta perlindungan yang optimal bagi masyarakat.

Seiring dengan berkembangnya teknologi Artificial Intelligence yang memungkinkan terjadinya pemalsuan wajah atau *Deepfake*, permasalahan hukum tidak hanya berhenti pada aspek pengaturan normatif semata, tetapi juga berlanjut pada bagaimana pertanggungjawaban pidana dapat dikenakan kepada pelaku. Hal ini menjadi penting mengingat karakteristik teknologi AI yang kompleks, yang dalam praktiknya dapat melibatkan berbagai pihak, baik sebagai pembuat, pengguna, maupun penyebar konten hasil manipulasi tersebut. Pertanggungjawaban pidana dalam konteks pemalsuan wajah berbasis AI menuntut adanya pembuktian mengenai unsur kesalahan, baik dalam bentuk kesengajaan maupun kelalaian, serta adanya perbuatan melawan hukum yang menimbulkan kerugian bagi pihak lain. Selain itu, perkembangan teknologi juga menimbulkan pertanyaan baru mengenai batasan pertanggungjawaban, khususnya ketika teknologi AI berperan sebagai alat yang secara otonom menghasilkan suatu konten tanpa intervensi langsung manusia secara penuh.

Dalam konteks hukum pidana, istilah pertanggungjawaban pidana dikenal dalam bahasa asing sebagai t*eorekenbaardheid atau criminal responsibility*, yang merujuk pada proses pemidanaan terhadap pelaku dengan penentuan pertanggungjawaban pelaku dalam suatu tindak pidana bertujuan untuk menilai apakah individu tersebut layak dimintai tanggung jawab secara hukum atas perbuatan yang dilakukannya. Suatu tindakan hanya dapat dijatuhi sanksi pidana apabila seluruh unsur-unsur yang membentuk tindak pidana sebagaimana ditetapkan dalam ketentuan perundang-undangan terpenuhi secara utuh dan menyeluruh. Apabila ditinjau melalui aspek hukum formal, individu hanya dapat dikenakan pidana apabila perbuatannya tergolong sebagai perbuatan melawan hukum dan tidak disertai dengan mengahaapuskan sifat melawan hukum yang dapat disebut sebagai alasan pembenar. Sementara itu, dari perspektif kemampuan bertanggung jawab, hanya individu yang secara hukum dianggap cakap dan mampu bertanggung jawab yang dapat dikenai pertanggungjawaban pidana. Oleh karena itu, pertanggungjawaban pidana tidak sebagatas berkaitan yang dilihat dari perbuatan yang diperbuat, akan tetapi menyangkut subjek hukum yang melakukannya dan kondisi-kondisi yang menyertai perbuatan tersebut. [16]

Dalam kaitannya dengan pemalsuan wajah berbasis teknologi *artificial intelligence* (AI), konsep pertanggungjawaban pidana menjadi semakin kompleks karena melibatkan penggunaan teknologi sebagai alat dalam melakukan tindak pidana. Meskipun AI memiliki kemampuan untuk menghasilkan konten secara otomatis, namun dalam perspektif hukum pidana, AI tidak dapat dipandang sebagai subjek hukum yang dapat dimintai pertanggungjawaban. Oleh karena itu, pertanggungjawaban tetap dibebankan kepada manusia sebagai pihak yang merancang, mengoperasikan, atau memanfaatkan teknologi tersebut untuk tujuan tertentu.[17]

Dalam hal ini, terdapat beberapa pihak yang berpotensi dimintai pertanggungjawaban pidana, yaitu pertama, pihak yang membuat atau mengembangkan konten *deepfake* dengan sengaja untuk tujuan melawan hukum; kedua, pihak yang menyebarluaskan atau mendistribusikan konten tersebut kepada publik; dan ketiga, pihak yang dengan sadar menggunakan konten *deepfake* untuk memperoleh keuntungan atau merugikan pihak lain. Penentuan pihak yang bertanggung jawab ini harus didasarkan pada peran serta dan kontribusi masing-masing dalam terjadinya tindak pidana. selanjutnya, untuk dapat menjerat pelaku dengan pertanggungjawaban pidana, harus dibuktikan adanya unsur kesalahan (*schuld*), baik dalam bentuk kesengajaan (*dolus*) maupun kelalaian (*culpa*). Dalam kasus pemalsuan wajah berbasis AI, kesengajaan dapat terlihat ketika pelaku secara sadar dan terencana menggunakan teknologi untuk membuat atau menyebarkan konten palsu yang merugikan orang lain, misalnya untuk melakukan penipuan atau pencemaran nama baik. Sementara itu, kelalaian dapat terjadi apabila seseorang menyebarkan konten tanpa melakukan verifikasi terlebih dahulu, padahal seharusnya ia dapat menduga bahwa konten tersebut merupakan hasil manipulasi.

---

[16] Wahyuni, F., 2017. *Dasar-dasar Hukum Pidana di Indonesia*. Tangerang Selatan: PT. Nusantara Persada Utama, hlm. 67

[17] Teguh Prasetyo, 2016. *Hukum Pidana*, Jakarta: Rajawali Pers, hlm. 67.

Selain itu, tidak kalah penting adalah adanya hubungan kausal antara perbuatan pelaku dengan akibat yang ditimbulkan. Dalam konteks ini, harus dapat dibuktikan bahwa kerugian yang dialami korban merupakan akibat langsung dari tindakan pelaku dalam membuat atau menyebarkan konten *deepfake*. Kerugian tersebut dapat berupa kerugian materiil, seperti kehilangan uang akibat penipuan, maupun kerugian immateriil, seperti rusaknya reputasi, tekanan psikologis, atau pelanggaran terhadap privasi. di sisi lain, dalam menentukan pertanggungjawaban pidana juga perlu diperhatikan kemungkinan adanya alasan pemaaf dan alasan pembenar. Alasan pembenar, seperti pembelaan terpaksa (*noodweer*), dapat menghapus sifat melawan hukum dari suatu perbuatan, sedangkan alasan pemaaf, seperti ketidakmampuan bertanggung jawab, dapat menghapus kesalahan pelaku. Namun, dalam praktiknya, penggunaan teknologi AI untuk pemalsuan wajah umumnya dilakukan secara sadar dan terencana, sehingga sulit untuk dibenarkan atau dimaafkan dalam kerangka hukum pidana.[18]

Dengan demikian, pertanggungjawaban pidana terhadap pelaku pemalsuan wajah berbasis teknologi AI pada dasarnya tetap mengacu pada prinsip-prinsip umum hukum pidana, namun memerlukan penafsiran yang lebih adaptif terhadap perkembangan teknologi. Hal ini penting agar hukum tetap mampu menjangkau berbagai bentuk kejahatan baru yang timbul akibat kemajuan teknologi, serta memberikan perlindungan hukum yang efektif bagi masyarakat.

B. Perlindungan Hukum Bagi Korban Pemalsuan Wajah yang Menggunakan Teknologi AI di Indonesia Sesuai dengan Sistem Hukum yang Berlaku

Perlindungan terhadap korban merupakan salah satu aspek yang harus diperhatikan dalam timbulnya perbuatan pidana, karena hak-hak korban merupakan sebuah elemen dalam konsep hak asasi manusia yang merupakan salah satu filosofi dari tujuan hukum pidana itu sendiri yaitu melindungi kepentingan individu dan kepentingan masyarakat.[19] Oleh sebab itu, jika hak asasi manusia terancam atau diganggu, korban harus dilindungi secara hukum serta haknya tidak boleh diambil secara langsung tanpa melalui adanya proses hukum. Konsep tersebut sebagai akibat dari sebuah negara hukum, dimana keberadaan sebagai negara hukum yang mementingkan hak-hak korban yang harus dilindungi melalui proses hukum.[20] Hukum adalah seperangkat aturan atau norma yang mengatur tingkah laku manusia sebagai makhluk sosial dalam kehidupan sehari-hari. Hukum biasanya berisikan norma-norma atau kaidah-kaidah hukum yang dibuat untuk mengatur tata tertib kehidupan dalam masyarakat.[21] Salah satu Upaya yang harus dilakukan oleh masyarakat adalah untuk menanggulangi dan memerangi kejahatan dengan Hukum Pidana. Penggunaan hukum pidana sangat penting digunakan sebagai dasar pencelaan atas perbuatan melanggar hukum yang dilakukan untuk mewujudkan keadilan, ketertiban dan kepastian hukum. Hukum Pidana merupakan sarana terakhir atau ultimum remedium bila sarana lain tidak cukup untuk melakukan penanggulangan suatu perbuatan tindak pidana.[22]

Di era teknologi ini hukum menjadi peran penting dalam mengatur dan melindungi masyarakat dari dampak digitalisasi. Salah satunya media sosial yang dimana sekarang menjadi tempat platform digital untuk beinteraksi, berbagi konten dan bersosialisasi secara online, seperti Instagram, twitter, facebook, tiktok whatsapp dan lain-lain. Media sosial banyak sekali melahirkan berbagai cara untuk berinteraksi, dengan melalui media sosial seseorang bisa berinteraksi dengan siapapun baik orang dalam negeri maupun luar negeri. Media sosial sering disalahgunakan oleh berbagai pihak salah satunya yaitu dijadikan sebagai media politik, propaganda, perundungan dan ujaran kebencian dengan tujuan untuk mencari keuntungan dan meraup dukungan dengan cara menyebarkan berita palsu dan informasi hoax sebagai jalan pintas untuk mencari keuntungan.[23] Teknologi komputer semakin baik dalam mensimulasikan realitas, seperti contohnya AI (artificial intelligence) atau kecerdasan buatan

[18] Andi Hamzah, 2010. *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, hlm. 134.

[19] Ayu Efritadewi, 2020. *Modul Hukum Pidana*, UMRAH Press, Tanjung Pinang, hlm. 4-5.

[20] Herlyanty Bawole, *Perlindungan Hukum Bagi Korban Dalam Sistem Peradilan Pidana*, Lex Et Societatis, 9. 3, Juli-September (2021), hlm. 17. https://ejournal.unsrat.ac.id/v3/index.php/lexetsocietes/article/view/36433.

[21] Yati Nurhayati, 2020. *Buku Ajar Pengantar Ilmu Hukum*, Bandung, Penerbit Nusa Media, hlm. 23-24

[22] Danrivanto Budhijanto, 2017. *Revolusi Cyber Law Indonesia Pembaharuan dan Revisi UU ITE 2016*, Bandung, PT Refika Aditama, hlm. 33

[23] Itsna Hidayatul Khusna Sri Pangestuti, *Deepfake, Tantangan Baru Untuk Netizen Deepfake, a New Challenge for Netizen*, AGUSTUS 1945 JAKARTA 1 PROMEDIA, no. 2 (2019): 1–24. https://doi.org/10.52447/promedia.v5i2.2300. 2019. hlm. 10-11

yang merancang teknologi *deepfake* AI, dan menjadi pusat perhatian masyarakat terutama dalam pembuatan video, gambar dan audio yang dirancang untuk meniru seseorang, membuatnya tampak seolah olah mereka melakukan sesuatu yang tidak mereka lakukan. Sebagaimana contoh kasus *Deepfake* yang menggunakan wajah bapak presiden Republik Indonesia, bapak Prabowo Subianto dimana Tersangka menggunakan teknologi AI (*Artificial Intelligence*) untuk membuat video palsu yang menampilkan wajah dan suara yang sangat mirip dengan Presiden Prabowo Subianto. Dalam video tersebut, sosok yang menyerupai Prabowo tampak berbicara seolah-olah sedang menawarkan bantuan pemerintah kepada masyarakat. Video palsu ini diunggah dan disebarluaskan di media sosial, terutama Instagram (salah satunya melalui akun bernama "Indo Berbagi 2025".

Tersangka mencantumkan nomor WhatsApp dalam video tersebut, mengarahkan korban yang tertarik untuk mengisi pendaftaran bantuan, dan meminta sejumlah uang sebagai biaya administrasi atau pendaftaran. Setelah uang ditransfer, bantuan yang dijanjikan tidak pernah ada. Hal ini bisa menyebabkan penyalahgunaan teknologi dalam era digitalisasi untuk mencari keuntungan pribadi atau kepentingan politik. Meskipun prosesnya rumit, perangkat lunaknya cukup mudah diakses, beberapa aplikasi yang memudahkan pembuatan *deepfake* antara lain yaitu DeepFace Lab, Fake App, Face Swap, dan sejumlah besar perangkat lunak *deepfake* dapat ditemukan di GitHub. GitHub adalah sebuah platform berbasis cloud yang dirancang untuk menyimpan, mengelola, dan mendokumentasikan kode sumber, serta memfasilitasi kolaborasi antar pengembang.

Secara konstitusional, Undang-Undang Dasar 1945 telah memberikan aturan dan jaminan terhadap penduduknya untuk mendapatkan perlindungan. Di dalam Pasal 28 D Ayat (1) menyatakan, “Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum.” Hukum seharusnya berada didepan dalam menumbuhkan lingkungan teknologi yang sehat. Hal tersebut dapat dilakukan dengan memperjelas substansi dari hukum positif dalam menggambarkan *deepfake* atau manipulasi objek menggunakan kecerdasan buatan (AI) kemudian memandu para pemangku kepentingan sebagai peran utama sebagai penetapan standar mengenai bagaimana kemampuan kecerdasan buatan *deepfake* dapat dibatasi. Dalam hukum pidana Indonesia AI *deepfake* disamakan dengan “Agen Elektronik” karena sifatnya dalam otomatisasi pemrosesan informasi. Dalam Pasal 1 UU ITE mendefinisikan, “Agen Elektronik” merupakan perangkat dari suatu “Sistem Elektronik”, yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang. Sehingga agen elektronik merupakan bagian dari sistem elektronik. Setiap penyelenggara, baik sistem elektronik maupun agen elektronik, bertanggung jawab untuk memastikan bahwa sistem yang mereka gunakan aman, dapat diandalkan, dan akuntabel. Hal ini dikarenakan penyelenggara agen elektronik memikul tanggung jawab penuh atas setiap konsekuensi hukum yang timbul dari penggunaan sistem tersebut, seperti yang diatur dalam Pasal 21 UU ITE Oleh sebab itu, peranan pengatur sangatlah penting dalam melindungi hak-hak masyarakat dan menyeimbangkan kemajuan teknologi artificial intelligence (AI) sekarang ini.

Hakikat dari kejahatan semestinya melihat sebagai bentuk sesuatu yang merugikan korban. Karena itu, bukan hanya memberikan sanksi pidana bagi pelanggar dalam konteks perbuatannya, namun juga memperhatikan kepentingan pemulihan terhadap korban yang bukan hanya berupa rehabilitasi, psikologis, dan ganti kerugian, tetapi juga memberikan tindakan solutif terhadap korban yang memiliki ketakutan dalam bermasyarakat sosial yang mengganggu korban dalam aktivitas dalam pekerjaannya. Hal ini tercantum di dalam Pasal 5 Undang-Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban. Selain itu, penyebaran *deepfake* juga berkaitan erat dengan perlindungan hak asasi manusia, khususnya hak atas privasi, kehormatan, dan martabat manusia. Ketika wajah atau suara seseorang dimanipulasi tanpa persetujuan dan disebarluaskan secara luas, maka terdapat pelanggaran serius terhadap hak personal individu. Oleh karena itu, negara memiliki kewajiban untuk menghadirkan instrumen hukum yang mampu memberikan perlindungan efektif serta menjamin keadilan bagi korban kejahatan berbasis *deepfake*

Kasus *deepfake* suara dan video menimbulkan tantangan hukum yang relevan dan kompleks bagi penyelidikan dan penuntutan kejahatan, sebab otoritas penegak hukum belum mempunyai kemampuan penuh untuk mengamankan bukti-bukti berskala internasional dan sering kali kurangnya kerangka hukum khususnya langkah-langkah prosedural dalam hukum pidana untuk memerintahkan pelestarian bukti digital dan menyelidiki kejahatan dunia

maya, hal tersebut merupakan hambatan besar dalam struktur penegakan hukum pidana terhadap terknologi artificial intelligence.

Karena kompleksitas yang ditimbulkan oleh penyalahgunaan teknologi artificial intelligence untuk tujuan kriminal, maka bagi lembaga penegak hukum dan para pemangku kepentingan utama atau pemerintah mesti berupaya untuk mendorong pengembangan kemitraan strategis antara penegak hukum untuk melawan penyalahgunaan dengan lebih efektif. Sehingga prospek untuk mengembangkan peraturan baru menjadi terobosan yang akan mengatur aspekaspek relevan mengenai dampak dan pengembangan sistem artificial intelligence dan bersinggungan dengan perlindungan hak-hak dasar bagi korban. Sebab "Indonesia merupakan negara yang menganut sistem hukum eropa kontinental, yang dimana segala tindakan dan perbuatan mesti memiliki aturan tertulis dalam menjalankan tujuan yaitu kepastian hukum".[24]

Peraturan hukum di Indonesia, khususnya hukum pidana atau undang-undang yang berkaitan dengan teknologi artificial intelligence sampai saat ini belum mengatur secara spesifik terkait artificial intelligence kedalam konsideran peraturan serta belum ada optimalisasi peraturan yang berkaitan dengan pengunaan artificial intelligence, yang mana hal ini bisa menjadi celah hukum bagi pelaku penyalagunaan teknologi artificial intelegence. Ketiadaan pengaturan khusus tersebut berpotensi menimbulkan kekosongan hukum (rechtsvacuum) maupun ketidakpastian hukum (legal uncertainty) dalam praktik penegakan hukum. Aparat penegak hukum sering kali harus melakukan penafsiran ekstensif terhadap norma yang ada untuk menjerat pelaku, yang pada akhirnya dapat menimbulkan perbedaan penerapan hukum antar kasus. Situasi ini menunjukkan bahwa hukum positif Indonesia masih menghadapi tantangan besar dalam mengimbangi perkembangan teknologi yang bergerak sangat cepat.

Sebagai negara hukum yang mengenal asas due proses of law, dimana segala sesuatu yang dilakukan atau perbuatan harus berdasarkan peraturan perundang undangan dan dalam hukum pidana pun menjelaskan penjatuhan hukuman pada seseorang tidak bias dilakukan tanpa adanya undang-undang yang mengaturnya (asas legalitas), maka dengan demikian masalah yang memiliki potensi lahirnya tidak pidana dan merugikan masyarakat diharuskan cepat teratasi dengan keberadaan hukum sebagai solusinya. Hukum pidana yang mengatur perilaku dalam kehidupan publik dan diberikan pemidanaan bilamana peraturan tersebut dilanggar. Hukum pidana memiliki dua pembagian hukum yaitu hukum pidana umum dan hukum pidana khusus yang masing-masing memiliki cakupan dan ruang lingkup tersendiri.

Dari pembagian hukum pidana tersebut, maka seharusnya keberadaan dan penggunaan teknologi artificial intelligence dimuat dan dibentuk dalam hukum pidana umum maupun pidana khusus atau dibuatkan suatu peraturan tentang teknologi artificial intelligence, baik secara spesifik dalam bentuk undang-undang atau bab tersendiri, seperti pembentukan tersebut dibuat dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik (UU ITE). Sebab pada dasarnya, jika tidak ada kesalahan maka tidak bisa dipidana sehingga hal ini menimbulkan pertanyaan apakah artificial intelligence dapat bertanggung jawab atas tindakannya sendiri atau bagaimana jika hasil dari pemikiran artificial intelligence menimbulkan tindak pidana, maka kemudian siapakah yang bertanggung jawab di mata hukum, apakah artificial intelligence atau pembuat artificial intelligence dan ataukah pengguna artificial intelligence itu sendiri.

Penyalahgunaan teknologi *deepfake* menimbulkan tantangan serius dalam konteks hukum dan etika. Kejahatan semacam ini merujuk pada ketentuan dalam Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Hal ini menimbulkan pertanyaan mengenai batasan hukum dalam menangani kasus-kasus *deepfake* dan bagaimana masyarakat serta individu dapat melindungi diri dari potensi penyalahgunaan teknologi ini.

Perlindungan terhadap korban merupakan salah satu aspek penting dalam timbulnya perbuatan pidana, hak-hak korban merupakan sebuah elemen dari tujuan hukum pidana itu sendiri yaitu melindungi kepentingan individu dan masyarakat. Oleh sebab itu korban harus dilindungi secara hukum, konsep tersebut sebagai akibat dari sebuah negara hukum yang mementingkan hak-hak korban harus dilindungi

[24] Abi Umaroh, 2023. *Pertumbuhan Artificial Intelegence Serta Implikasinya Terhadap Hukum Dan Etika Ham (Salah Tangkap Pelaku Kriminal Menggunakan Teknologi Face Recognition)*, Deposisi: Jurnal Publikasi Ilmu Hukum, Vol. 1, No. 3, hlm. 262–273.

melalui proses hukum.[25] Perbuatan yang dilakukan oleh pelaku kejahatan yang bertentangan dengan hukum akan menimbulkan ganti kerugian terhadap korban seperti kompensasi, restitusi dan sebagainya. Dalam membuat kebijakan hukum, negara harus memberikan kepastian hukum dan persamaan hak-hak manusia dalam regulasi aturan hukum pidana, baik aturan yang bersifat secara khusus maupun secara umum dengan tujuan untuk menjaga ketertiban dan kenyamanan dalam masyarakat. Kedudukan orang perorangan tidak lepas dari aktivitas pemanfaatan teknologi di dunia maya, Kebijaksanaan hukum menjadi prioritas utama untuk membuat ketertiban yang ada di dalam masyarakat, kemajuan teknologi merupakan hal yang menjadi bagian dari pada masyarakat. [26]Kebijaksanaan yang dimaksud adalah kebijaksanaan hukum atas perlindungan huku terhadap hak-hak yang ada pada korban. Korban berhak atas segala hak, baik itu hak atas perlindungan, hak representasi, hak atas reparasi dan hak atas partisipasi. Hak atas perlindungan meliputi hak yang diperuntukkan terhadap korban untuk mendapatkan perlindungan fisik maupun mental. Hak representasi merujuk kepada hak untuk didengarkan keteranganny sesuai dengan yang dia alami. Hak reparasi adalah hak yang menyangkut kompensasi dan resititusi korban untuk memperoleh kerugian dari negara dan pelaku. Hak atas partisipasi artinya hak ikut serta dalam menentukan bentuk perlindungan dari negara. Korban berhak atas semua hak-hak mereka untuk diperlakukan dengan rasa kasi dan menghormati martabatnya[27].

Peranan dan kapasitas hukum sebagai instrumen social engineering yang bertujuan untuk mencapai ketertiban serta kesadaran hukum dalam masyarakat sebagaimana cita-cita hukum dan sekaligus bersifat responsif terhadap perubahan-perubahan sosial dan peranannya sebagai sarana social control yang mengupayakan ketertiban hukum atau strategi dalam mencegah perilaku melanggar serta menyimpang dalam kehidupan masyarakat. Hal ini selaras dengan asas ius konstitutum sebagai hukum positif yang berlaku saat ini dan ius konstituendum sebagai hukum yang direncanakan atau dicita-citakan, beberapa hal tersebut menggambarkan sifat hukum, dimana hukum menjadi faktor penentu kehidupan masyarakat dan dimana hukum menyesuaikan dengan perkembangan dari masyarakat itu sendiri, baik perkembangan sosial maupun teknologi. Sebagai Negara yang berkonsepsi negara hukum, dimana dalam konstitusinya yang tertuang melalui Pasal 1 ayat (3) Undang-Undang Dasar 1945 mengatakan "Indonesia adalah negara hukum", yang menjelaskan pengakuan normatif tentang segala sesuatu atau peristiwa yang diharuskan mengikuti tatanan peraturan yang sudah diresmikan oleh negara sebagai pedoman berperilaku dalam negara.

Dalam konteks *deepfake* peraturan yang ada di Indonesia, belum sepenuhnya efektif melindungi korban dan memberikan efek jera terhadap pelaku dikarenakan adanya ketidakjelasan makna mengenai *deepfake* itu sendiri di dalam hukum. Penegakan hukum yang ada sering kali tidak sejalan dengan kemajuan teknologi yang begitu pesat, aturan yang ada hanya sebatas mencegah dan tidak memberikan efek jera terhadap pelaku karena belum bersifat tegas dan mengikat pelaku penyalahgunaan teknologi AI, ini menimbulkan permasalahan hukum baru yang bisa memperburuk situasi. Sehingga diperlukan adanya urgensi pengaturan mengenai *deepfake* AI ini, yaitu dengan dilakukannya aturan yang bersifat khusus atau melakukan perbaikan dan pembuatan aturan mengenai penyalahgunaan artificial intelligence yang memuat ketentuan secara jelas dan mengikat pelaku dari perbuatan penyimpangan. Sehingga akan tercipta kepastian hukum dan perlindungan hukum terhadap korban dari penyalahgunaan teknologi *deepfake* AI. Indonesia seharusnya sudah memiliki aturan ini dan melakukan pembaharuan hukum dengan melihat substansi hukum itu sendiri yang dimulai dari struktur, segi hukum, kebutuhan hukum yang ada di masyarakat dan sebagainya. Hal ini memilki tujuan untuk mengantisipasi penggunaan teknologi *deepfake* AI secara berlebihan serta sebagai suatu sistem kontrol dalam penggunaan keccerdasan buatan tersebut.

PENUTUP

A. Kesimpulan

1. Meskipun hingga saat ini Indonesia belum memiliki regulasi yang secara khusus mengatur tentang pemalsuan wajah berbasis AI, berbagai ketentuan dalam peraturan perundang-undangan yang berlaku telah memberikan landasan normative untuk menindak pelaku. Ketentuan dalam kitab undang-undang hokum pidana (KUHP) dapat

[25] Ayu Efritadewi, 2020. *Modul Hukum Pidana*, UMRAH Press, Tanjung Pinang, hlm 86

[26] Budi Sastra Panjaitan, 2022. *Viktimologi Pandangan Advokat Terhadap Perbuatan Pidana dan Korban,* Banyumas: CV. Amerta Media, hlm. 6

[27] Mahrus Ali, 2020. *Viktimologi*, Depok: PT Raja Grafindo Persada, hlm. 21

digunakan untuk menjerat perbuatan yang mengandung unsur penipuan, pencemaran nama baik, maupun penyebaran berita bohong. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memberikan pengaturan yang lebih spesifik terkait perbuatan yang dilakukan melalui media elektronik, termasuk penyebaran konten yang melanggar hukum, seperti penghinaan, pelanggaran kesusilaan, dan penyebaran informasi yang merugikan masyarakat. Sementara itu, Undang-Undang Perlindungan Data Pribadi (UU PDP) juga memiliki relevansi yang signifikan, mengingat penggunaan data biometrik seperti wajah dan suara dalam teknologi *deepfake* merupakan bagian dari data pribadi yang harus dilindungi dan tidak dapat diproses tanpa persetujuan dari subjek data.

2. Perlindungan hukum terhadap korban pemalsuan wajah melalui teknologi kecerdasan buatan (AI) berbasis *deepfake* di Indonesia pada tahap ini masih bersifat fragmentaris dan normatif umum, mengandalkan kerangka regulasi yang ada seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru), serta Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Ketentuan-ketentuan ini, meskipun relevan, belum secara eksplisit mengkategorikan *deepfake* sebagai delik pidana tersendiri, sehingga penegak hukum kerap melakukan interpretasi ekstensif terhadap pasal-pasal seperti Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik elektronik, Pasal 378 KUHP tentang penipuan, atau Pasal 32 UU PDP mengenai penyalahgunaan data pribadi.

B. Saran

1. Diperlukan pembentukan regulasi khusus yang secara eksplisit mengatur penggunaan dan penyalahgunaan teknologi Artificial Intelligence, khususnya terkait dengan praktik *deepfake*. Ketentuan yang saat ini masih bersifat fragmentaris dalam KUHP, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi, belum sepenuhnya mampu menjawab kompleksitas kejahatan berbasis AI. Oleh karena itu, pembentuk undang-undang perlu merumuskan norma hukum yang lebih komprehensif, termasuk definisi yuridis mengenai *deepfake*, klasifikasi perbuatan yang dilarang, serta mekanisme pembuktian yang adaptif terhadap karakter digital.
2. Negara perlu memastikan implementasi hak-hak korban secara optimal, seperti hak atas perlindungan, hak atas pemulihan (restitusi dan kompensasi), serta hak atas rehabilitasi psikologis. Selain itu, perlu dikembangkan mekanisme yang efektif untuk pemulihan reputasi korban di ruang digital, termasuk penghapusan konten (take down mechanism) secara cepat dan tepat. aparat penegak hukum perlu meningkatkan kapasitas dan kompetensi dalam menangani kejahatan berbasis teknologi digital, khususnya yang berkaitan dengan *deepfake*.

DAFTAR PUSTAKA

Buku

Ayu Efritadewi, 2020. Modul Hukum Pidana, UMRAH Press, Tanjung Pinang.

Budi Sastra Panjaitan, 2022. "Viktimologi Pandangan Advokat Terhadap Perbuatan Pidana dan Korban, Banyumas.

Edmon Makarim, 2020. *Pengantar Hukum Telematika*, Jakarta.

Agus Mulyanto, 2020. *Sistem Keamanan Jaringan Komputer*, Yogyakarta.

Edi S. Mulyanta, 2020. *Pengenalan Artificial Intelligence dan Machine Learning*, Yogyakarta.

Doni Nurdiansyah, 2024. *Kecerdasan Buatan dalam Pendidikan*, Deepublish, Yogyakarta.

H Budhi, I gusti Kade, 2022. Artificial Intelligence Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana. Rajawali Pers.

Ir. M. Salim, Sulistiawati Rahayu N. Ahmad, Mardhiyah Hayati, Muhammad Diponegoro, Yusril Eka Mahendra, 2024. *Hukum dan Teknologi Informasi*, Yayasan Tri Edukasi Ilmiah.

Jamaaluddin & Indah Sulistyowati, 2021. *Buku Ajar Mata Kuliah Kecerdasan Buatan (Artificial Intelligence)*, Umsida Press, Sidoarjo.

Kaharuddin dan Zul Amirul Haq, 2024. *Kecerdasan Buatan: Aspek Perlindungan Hukum*.

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

Mahrus Ali, 2020. VIKTIMOLOGI, Depok, PT Raja Grafindo Persada.

Nurlita, S. 2025. Implikasi Legal dari *Deepfake*: Ganti Rugi Perdata atas Pemalsuan Wajah dan Suara. Al-Zayn: Jurnal Ilmu Sosial & Hukum.

Safitri, A. D. & Zuhriyah, K. 2025. Pengertian Tindak Pidana dan Unsur-Unsurnya.

Usman Ependi & Albertus Dwiyoga Widiantoro (Ed.), 2024. *Buku Ajar Kecerdasan Buatan*, Asosiasi Doktor Sistem Informasi Indonesia (ADSII).

Yusuf, Anselmus. 2010. Metodologi Penelitian Hukum. Bandung: Refika Aditama.

Peraturan Perundang-Undangan

Undang-undang Dasar Negara Republik Indonesia 1945

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Jurnal / Artikel /Penulisan Ilmiah

Haida, Rendi Syaputra Nur, dan Eko Nuriyatman. "Urgensi Pengaturan Perlindungan Hukum terhadap Korban *Deepfake* di Indonesia." Jurnal Hukum Respublica Vol. 23, No. 2 (2023): 113–115.

Afni, N. (2024). Pengaturan Hukum terhadap Tindak Pidana Penyalahgunaan Teknologi AI dalam Kejahatan Voice Phishing. Jurnal Hukum De Rechtsstaat, Vol. 10, No. 2.

Chesney, Robert, dan Danielle K. Citron. (2019). *Deepfake*: Tantangan Serius bagi Privasi, Demokrasi, dan Keamanan Nasional. California Law Review, Vol. 107, No. 6, hlm. 1753–1820.

Declaration of Independence. (1776). Deklarasi Kemerdekaan Amerika Serikat: Prinsip Hak Asasi Manusia yang Melekat secara Inheren pada Setiap Individu.

Anfa'un Nisa'.F.R., Syariffudin., et al., 2025, Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik *Deepfake*, Perspektif Administrasi Publik dan Hukum, Vol. 2, No. 1, hlm. 250.

Goodfellow, Ian, dkk. (2020). Generative Adversarial Networks (GAN): Konsep dan Perkembangannya. Communications of the ACM, Vol. 63, No. 11, hlm. 139–144.

Haris, Muhammad Tan Abdul Rahman, dan Tantimin Tantimin. "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence di Indonesia." Jurnal Komunikasi Hukum (JKH). Volume 8. No. 1 (2022). Halaman 307-316

Kietzmann, Jan, dkk. (2020). *Deepfake*: Tipuan atau Ancaman? *Business Horizons*, Vol. 63, No. 2, hlm. 135–146.

Marzuki, Peter Mahmud. Penelitian Hukum. Jakarta: Kencana Prenada Media Group, 2011.

Russell, Stuart, dan Peter Norvig. (2021). Kecerdasan Buatan: Pendekatan Modern (Edisi ke-4). Harlow: Pearson.

Herlyanty Bawole, "Perlindungan Hukum Bagi Korban Dalam Sistem Peradilan Pidana," LexEtSocietatis, 9. 3, Juli-September (2021), hlm. 17. https://ejournal.unsrat.ac.id/v3/index.php/lexetsocietes/article/view/36433.

Hukum di Era Globalisasi. Kencana.

Website

Direktorat Tindak Pidana Siber Bareskrim Polri. (2022). Laporan Kasus Pemalsuan Wajah Digital. Direktorat Tindak Pidana Siber Bareskrim Polri. (2022). Laporan Kasus Pemalsuan Wajah Digital. - Search.