JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI:https://doi.org/10.38035/jihhp.v6i1

Pertanggung Jawaban Pidana Terhadap Rekayasa Foto yang Mengandung Unsur Pencemaran Nama Baik

Fajar Nurshall Herianto[1].
[1]Universitas Al Azhar Indonesia, Indonesia, nurshallf@gmail.com.

Corresponding Author: nurshallf@gmail.com [1]

Abstract: *As artificial intelligence (AI) technology has grown, it has changed many aspects of human life. However, it has also brought about new problems, such as digital crime and deepfake technology. This technology is often misused to create defamatory content, particularly by superimposing an individual's face onto pornographic photos or videos and then distributing it via the internet. This trend makes it very hard to protect people's right to privacy and respect in the digital age. The point of this study is to look into the different types of criminal responsibility that people who change photos in a way that hurts others can face, as well as the good laws that can be used to punish offenders and protect victims. This research looks at the theory of criminal liability to figure out who is legally responsible in this case. It uses a normative legal research method with a statutory and conceptual approach. The results show that spreading false and damaging deepfake content can be punished under Article 27 paragraphs (1) and (3) along with Article 45 of Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), Article 310 of the Criminal Code, and Article 66 of Law Number 27 of 2022 on Personal Data Protection. In addition to criminal liability, victims can also file civil lawsuits based on unlawful acts as stipulated in Article 1365 of the Civil Code. Law enforcement against this crime faces technical challenges, such as the difficulty of tracking perpetrators and proving the authenticity of content, thus requiring special regulatory support and cross-sectoral cooperation.*

Keywords: *photo manipulation, defamation, criminal liability, internet media, ITE Law*

Abstrak: Kemajuan dalam kecerdasan buatan (AI) sudah memengaruhi berbagai sisi kehidupan kita, tetapi juga menimbulkan masalah baru, seperti kejahatan siber, salah satunya melalui teknologi *deepfake*. Penyalahgunaan teknologi ini sering kali digunakan untuk menciptakan konten yang mengandung unsur pencemaran nama baik, terutama dengan menempelkan wajah individu ke dalam foto atau video bermuatan pornografi, lalu disebarkan melalui media internet. Fenomena ini menimbulkan persoalan serius dalam perlindungan hak privasi dan kehormatan individu di era digital. Riset ini bertujuan menganalisis bentuk pertanggungjawaban pidana terhadap oknum penyunting gambar yang bersifat memfitnah dan menelusuri landasan hukum positif Indonesia yang bisa dipakai guna menjerat pelaku serta memberikan perlindungan kepada korban. Riset ini menggunakan metode normatif dalam menggali hukumnya dan dengan pendekatan perundang-undangan serta pendekatan konseptual, serta mengkaji teori pertanggungjawaban pidana untuk menganalisis Pertanggung

Jawaban Pidana Terhadap Rekayasa Foto Yang Mengandung Unsur Pencemaran Nama Baik. Hasil penelitian menunjukkan bahwa penyebaran konten deepfake yang mencemarkan nama baik dapat dijerat melalui ketentuan Pasal 27 ayat (1) dan (3) jo. Pasal 45 UU No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (UU ITE) mengatur tentang larangan mendistribusikan atau mentransmisikan konten yang melanggar kesusilaan dan pencemaran nama baik melalui media elektronik, Pasal 310 KUHP mengatur tentang pencemaran nama baik, serta Pasal 66 UU No.27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur tentang sanksi pidana bagi setiap orang yang dengan sengaja membuat data pribadi palsu atau memalsukan data pribadi. Pasal 1365 KUHPer menyatakan korban perbuatan melawan hukum juga dapat mengajukan gugatan perdata selain gugatan pidana. Penegakan hukum terhadap kejahatan ini menghadapi tantangan teknis, seperti sulitnya pelacakan pelaku dan pembuktian keaslian konten, sehingga memerlukan dukungan regulasi khusus dan kerja sama lintas sektor.

Kata kunci: rekayasa foto, pencemaran nama baik, pertanggungjawaban pidana, media internet, UU ITE

PENDAHULUAN

Saat ini, ketika dunia semakin terhubung, teknologi dan media elektronik terus berkembang. Dengan munculnya layanan internet dan globalisasi teknologi, dunia telah menjadi era cyber. Layanan ini telah menciptakan dunia baru yang disebut dunia cyber yang menawarkan banyak manfaat dalam bentuk virtualnya. Perkembangan baru dalam bidang elektronik dan teknologi informasi sejatinya membawa harapan besar bagi peningkatan taraf hidup masyarakat. Inovasi-inovasi tersebut telah mempermudah akses terhadap informasi, mempercepat komunikasi, serta membuka peluang baru bagi pertumbuhan industri digital. Dalam banyak aspek, teknologi telah menjadi katalisator bagi transformasi sosial yang lebih inklusif dan dinamis. (Suryokencono, P., & Isyraq, R. F. (2024). Namun, kemajuan teknologi yang cepat juga menimbulkan dampak negatif seperti kejahatan siber, penyebaran informasi palsu, pelanggaran privasi, dan ketimpangan digital. Tanpa pengelolaan yang bijak serta dukungan kebijakan dan literasi digital, kemajuan ini dapat memperburuk kesenjangan sosial dan menghambat pembangunan

Di dunia modern, teknologi informasi dan komunikasi telah menghasilkan peningkatan dalam hal kecepatan dan kemudahan komunikasi antarmanusia, pengumpulan dan penyebaran data, serta penghapusan hambatan ruang dan waktu. Perubahan-perubahan ini telah membuka jalan bagi kebangkitan modernisasi yang terjadi di setiap negara. Komputer kini digunakan di hampir setiap lapisan masyarakat. Teknologi terbaru yang sedang berkembang adalah Artificial Intelligence (AI). (Nugroho, T. A., Amarco, A. K., & Yasin, M. (2023).

Teknologi merupakan bagian penting dari kehidupan sehari-hari. Meskipun ada banyak hal baik tentang kemajuan teknologi, kejahatan jelas meningkat, dan jenis-jenis kejahatan baru terus bermunculan. Oleh karenanya, masyarakat perlu berhati-hati dengan teknologi baru karena teknologi dapat dengan mudah menjadi tempat berkembang biaknya kejahatan. (Mansur, Arief, D. M., & Gultom, E. (2005). Semakin banyak kejahatan yang dilakukan dengan menyalahgunakan teknologi informasi. Jenis kejahatan dan cara melakukannya juga selalu berubah. Di sisi lain, penggunaan teknologi untuk menemukan pelaku kejahatan ini masih belum efektif. Tentu saja, hal ini sangat menakutkan bagi kebanyakan orang. Banyak kerugian finansial yang ditimbulkan akibat penipuan berbasis teknologi ini, dengan jumlah uang yang hilang mencapai angka yang sangat signifikan. Dalam beberapa tahun terakhir, jenis-jenis kejahatan digital mengalami peningkatan baik dari segi kuantitas maupun kompleksitas. Kemajuan teknologi komputer, yang semestinya digunakan untuk meningkatkan

keamanan dan efisiensi sistem, digunakan oleh pelaku kejahatan untuk menyusun aksi yang lebih rumit dan sulit diungkap.

Artificial Intelligence (AI) ialah langkah maju yang besar dalam perkembangan manusia. Pada tahun 1955, seorang ilmuwan Amerika bernama John McCarthy adalah orang pertama yang mengusulkan AI. AI telah berkembang pesat dan kini digunakan di banyak bidang kehidupan manusia. Banyak situs besar, seperti Amazon dan Facebook, sudah memakai AI gna membuat fitur yang dapat mengenali wajah. Google Translate dan bahkan mobil yang dapat mengemudi sendiri adalah beberapa fitur lainnya. Teknologi deepfake adalah teknologi baru yang muncul karena AI semakin canggih. (Kasita, I. D. (2022). Teknologi AI ini berasal dari kemajuan dalam kecerdasan buatan yang dirancang khusus untuk mengubah atau menciptakan gambar maupun video dari suatu objek atau peristiwa. Proses ini dilakukan melalui metode deep learning (pembelajaran mendalam), yang memungkinkan sistem untuk mempelajari dan meniru pola visual dari ribuan bahkan jutaan gambar dasar manusia. Dengan cara ini, AI dapat menghasilkan representasi visual yang sangat realistis, seolah-olah menggambarkan kejadian nyata, padahal sepenuhnya direkayasa secara digital. Teknologi ini dikenal luas dalam praktik deepfake, di mana wajah, suara, atau ekspresi seseorang dapat dimanipulasi dengan sangat halus dan meyakinkan. (Prayoga, H., & Tuasikal, H. (2025).

Teknologi AI ini awalnya digunakan untuk bersenang-senang. AI dapat menganimasikan foto sehingga karakter dalam foto tampak hidup. (Prayoga, H., & Tuasikal, H. (2025). Sayangnya, karena aplikasi berbasis AI begitu mudah didapatkan, aplikasi ini telah digunakan dengan berbagai cara yang tidak bermoral dan ceroboh dari waktu ke waktu, sama seperti teknologi lainnya. AI ini memungkinkan pengguna untuk mengubah foto dan video yang menampilkan wajah seseorang sesuka hati. (Prayoga, H., & Tuasikal, H. (2025). Misalnya, teknologi AI dapat disalahgunakan untuk melakukan berbagai tindakan yang merugikan, seperti penipuan digital, penyebaran berita palsu (hoaks), dan bahkan manipulasi materi seksual yang tidak etis. Dalam kasus penipuan, AI bisa digunakan untuk meniru suara atau wajah seseorang guna mengelabui korban melalui rekaman atau panggilan palsu. Penyebaran informasi palsu melalui video atau gambar yang dimanipulasi juga dapat memicu kepanikan, membentuk opini publik yang keliru, atau merusak reputasi individu maupun institusi. (Ramadhani, R. A., Rahman, S., & Bima, M. R. (2024).

Ada juga laporan penyalahgunaan konten menggunakan teknologi AI di Indonesia. Tokoh-tokoh terkenal seperti Syahrini dan Nagita Slavina telah terdampak, begitu pula orang-orang biasa. Pengguna Twitter terkejut ketika tren baru muncul yang menawarkan layanan untuk mengedit foto dan video seksual memakai wajah seseorang. (Utawi, E. i., & Ruhaeni, N. (2023). Pengguna Twitter yang ingin memakai layanan ini hanya perlu mengeklik *link* yang diberikan dan mengisi informasi tentang korban yang ingin mereka gunakan. Semua pertumbuhan dan penyebaran berlangsung secara pesat. Orang-orang bisa dirugikan oleh teknologi *deepfake* dalam berbagai cara, termasuk penyalahgunaan informasi pribadi, penyebaran informasi yang tidak pantas, penyuntingan dan pemalsuan data, serta fitnah. Semua orang tahu betapa berharganya nama baik dan betapa pentingnya melindungi dan menjaganya.

Penulis studi ini membahas sejumlah studi terkait, yakni:

Pertama, Penelitian yang dilakukan oleh Adzhar Anugerah Trunapasha, Pan Lindawaty Suherman Sewu, Dian Narwastuty, dan Shelly Kurniawan dengan judul *"Penyalahgunaan AI terhadap Tokoh Masyarakat dalam Konten di Media Sosial Berdasarkan Perundang-Undangan di Indonesia"* membahas mengenai bagaimana teknologi kecerdasan buatan, khususnya *deepfake* dan manipulasi digital, dapat digunakan untuk menyebarkan konten yang merugikan tokoh masyarakat melalui media sosial. Dalam penelitian tersebut, para penulis menganalisis aspek hukum positif Indonesia yang dapat dikenakan terhadap pelaku penyalahgunaan AI, serta mengkaji efektivitas regulasi yang ada dalam memberikan perlindungan hukum terhadap korban manipulasi konten digital. Riset ini ialah langkah besar

untuk memahami betapa pentingnya mengubah hukum dengan cepat di era digital yang semakin kompleks ini. (Trunapasha, A. A., Sewu, P. L. S., Narwastuty, D., & Kurniawan, S. (2023).

Kedua, Penelitian yang dilakukan oleh Pramukhtiko Suryokencono dengan judul *"Perlindungan Hukum Berupa Pemulihan Nama Baik Terhadap Korban Tindak Pencemaran Nama Baik Melalui Situs Deepfake"* menyoroti bentuk perlindungan hukum yang tersedia bagi individu yang menjadi korban pencemaran nama baik akibat penyebaran konten deepfake. Penelitian ini secara khusus mengkaji mekanisme pemulihan nama baik, baik melalui jalur perdata maupun pidana, serta mengkritisi keterbatasan regulasi yang ada dalam mengakomodasi perkembangan teknologi digital seperti deepfake. Hasil riset ini memperjelas betapa pentingnya mengubah hukum agar masyarakat korban penyalahgunaan digital memiliki rasa aman yang lebih. (Suryokencono, P. ., & Fakhrusy Isyraq , R. . (2025).

Ketiga, Penelitian yang relevan dengan penelitian ini dengan judul Pertanggungjawaban Pidana (Studi Putusan Nomor 1481/Pid.sus/2020/PN-Mks) yang dilakukan oleh A. Nurlatifah dkk menganalisis putusan pengadilan terkait pencemaran nama baik via media sosial, memeriksa kesesuaian unsur Pasal 27 UU ITE sebagai *lex specialis* dari KUHP, Penelitian menggarisbawahi bahwa UU ITE khususnya Pasal 27 berfungsi sebagai *lex specialis* (aturan khusus) yang mengatur pencemaran nama baik di ranah digital dengan lebih spesifik dibandingkan KUHP yang bersifat umum. UU ITE memungkinkan penegakan hukum dengan lebih tepat terhadap kejahatan berbasis media elektronik. (Nurlatifah, A., Thalib, H., & Khalid, H. (2021).

UU No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik di Indonesia dapat digunakan untuk mengadili orang yang melakukan tindak pidana pencemaran nama baik di internet. Selain itu, masalah muncul ketika seseorang mengambil gambar atau mengubahnya tanpa mencantumkan nama pemilik hak cipta, yang bertentangan dengan UU No.28 Tahun 2014 mengenai Hak Cipta. Mengubah gambar pribadi boleh saja, tetapi menjadi masalah jika digunakan untuk kegiatan ilegal atau merugikan orang lain. Permasalahan utama dalam kasus ini ialah undang-undang tersebut telah dilanggar beberapa kali. Oleh karenanya, diperlukan peninjauan yang lebih mendalam pada pelanggaran tindakan pembuatan gambar dengan konten yang mencemarkan nama baik.

Penelitian ini menawarkan kontribusi baru dengan memfokuskan analisis pada pertanggungjawaban pidana pelaku rekayasa foto berbasis *Artificial Intelligence (deepfake)* yang digunakan sebagai sarana pencemaran nama baik di media digital. Berbeda dengan studi terdahulu yang umumnya membahas pencemaran nama baik secara umum di media sosial, penelitian ini secara khusus mengkaji modus rekayasa foto, mengintegrasikan analisis Pasal 27 UU ITE sebagai *lex specialis* dari KUHP, dan mempertimbangkan potensi pelanggaran UU Hak Cipta. Selain itu, penelitian ini menyoroti kekosongan regulasi terhadap kejahatan berbasis AI serta menawarkan rekomendasi pembaruan hukum guna menyesuaikan dengan perkembangan teknologi informasi terkini.

Oleh karenanya, diperlukan riset yang lebih mendalam guna mendapatkan gambaran yang jelas dan langkah-langkah yang harus diambil untuk menggunakan hukum pidana guna menghentikan kejahatan teknologi dan informasi ini. Berkaca pada fenomena tersebut, penulis hendak mengulas secara khusus mengenai Bagaimana bentuk tanggung jawab hukum terhadap korban penyalahgunaan *Artificial Intelligence* terkhususnya teknik *Deepfake* dalam kejahatan pencemaran nama baik, maka dari itu, penulis memutuskan untuk menelaah persoalan ini dengan judul "Pertanggung Jawaban Pidana Terhadap Rekayasa Foto Yang Mengandung Unsur Pencemaran Nama Baik.

METODE

Riset ini menggunakan jenis penelitiian hukum normatif dan disusun dengan metode hukum. Metode memakai mengkaji UU No.1 Tahun 1946 KUHP, dan UU No.1 Tahun 2024, yang merupakan Perubahan ke 2 atas UU No.11 Tahun 2008, yang merupakan ITE. Penulis juga memakai metode konseptual yang didasarkan pada gagasan dan pandangan baru di bidang ilmu hukum. (Marzuki, P. M. (2021).

Sumber Hukum Primer Kitab Undang-Undang Hukum Pidana (KUHP) *Undang-Undang Nomor 1 Tahun 1946* tentang Peraturan Hukum Pidana beserta perubahannya, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta terkait perlindungan hak cipta pada gambar atau foto. Data yang telah dikumpulkan dalam penelitian ini dianalisis menggunakan metode analisis kualitatif dengan pendekatan deskriptif-analitis. Metode ini digunakan untuk menggambarkan secara sistematis fakta dan peraturan perundang-undangan yang berkaitan dengan penelitian tersebut.

Teori mengenai pertanggungjawaban pidana inilah yang digunakan dalam penelitian ini. Bertanggung Jawab atas Kejahatan. Istilah untuk tanggung jawab pidana dalam bahasa lain adalah "*toerekenbaarheid*", "*criminal responsibility*", dan "*criminal liability*". Tanggung jawab pidana ialah gagasan bahwa seorang tersangka atau penjahat harus bertanggung jawab atas kejahatan yang telah terjadi. Artinya, apakah pelaku akan dinyatakan bersalah atau tidak bersalah. Jika seseorang dinyatakan bersalah, harus jelas perbuatannya salah dan bahwa mereka dapat dimintai pertanggungjawaban. Keterampilan ini menunjukkan kesalahan orang yang melakukan kesalahan tersebut, baik sengaja maupun tidak sengaja. Jika terdakwa mengetahui perbuatan tersebut, berarti perbuatan tersebut salah. (Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024).

HASIL DAN PEMBAHASAN

Dinamika Penggunaan Deepfake Yang Merusak Reputasi Individu Dalam Ketentuan-Ketentuan Pidana

Artificial intelligence (AI) ialah studi tentang Pembuatan komputer yang mampu meniru kemampuan manusia, seperti berpikir dan belajar. Contohnya termasuk pembelajaran mesin, pembelajaran mendalam, jaringan saraf buatan, dan pengolahan bahasa manusia oleh komputer, dan istilah lainnya, semuanya digunakan untuk membicarakan *Artificial intelligence* (AI). AI (*Artificial intelligence*) telah memberikan dampak besar di banyak bidang, seperti perawatan kesehatan, pengenalan suara dan wajah, serta mobil tanpa pengemudi. Dalam beberapa kasus, AI telah digunakan di perusahaan swasta untuk menghasilkan uang bagi pemiliknya

Salah satu contoh dari bentuk AI adalah aplikasi *deepfake*. Deepfake ialah ide antarmuka pengguna yang dibuat oleh AI dan menggabungkan fitur wajah dengan gambar dan video agar terlihat lebih nyata. *Deepfake* menggunakan teknik pembelajaran mesin yang didasarkan pada cara kerja otak. *Deepfake* merupakan aplikasi dengan teknologi AI yang disalahgunakan oleh seseorang untuk melakukan perubahan video, gambar dan suara. *Deepfake* dapat digunakan untuk membuat video yang menyesatkan atau menipu, yang dapat berdampak negatif pada individu dan masyarakat. (Situmeang, B. S., Silitonga, I. Y., Silaen, R. F., Siringoringo, T. H., & Sipayung, E. E. (2024).

Temuan riset memperlihatkan teknologi *deepfake* memiliki dampak besar di banyak bidang. Penyalahgunaan utamanya adalah untuk pelecehan, penyebaran informasi palsu tentang politik, dan penipuan di sektor keuangan. Melalui analisis konten dan studi kasus, ditemukan bahwa *deepfake* sering digunakan untuk membuat konten seksual yang ditujukan kepada orang-orang tertentu, kebanyakan perempuan, untuk merusak nama baik dan citra

mereka. Sekitar 47% penyalahgunaan *deepfake* berkaitan langsung dengan kasus pelecehan pribadi, yang berdampak serius pada kehidupan sosial korban serta kesehatan mental mereka, terkadang menyebabkan trauma mendalam. Selain itu, teknologi ini juga dipakai guna menyebarkan kebohongan dan informasi palsu, terutama tentang politik. (Kurniawan, A. A., & Mustikasari, M. (2020).

Dalam sekitar 32% kasus yang diteliti, video rekayasa politisi yang memberikan komentar kontroversial digunakan untuk mengubah pikiran masyarakat menggunakan *deepfake.* Ini merupakan masalah besar menjelang pemilu 2024 di Indonesia. Teknologi *deepfake* berbasis audio juga telah digunakan untuk berpura-pura menjadi suara para pemimpin bisnis untuk melakukan penipuan, terutama ketika melakukan bisnis ilegal. Sekitar 21% dari semua kasus penyalahgunaan *deepfak*e yang telah diteliti merupakan jenis kejahatan ini. Hal ini dapat mengakibatkan kerugian finansial yang besar, terutama di dunia bisnis. (Kurniawan, A. A., & Mustikasari, M. (2020).

Hasil studi menunjukkan teknologi *deepfake* ialah ancaman yang sangat nyata bagi banyak aspek masyarakat, politik, dan ekonomi. Penyalahgunaan teknologi *deepfake* untuk tujuan pelecehan merupakan permasalahan serius yang semakin mengkhawatirkan. Dengan teknologi ini, penjahat dapat mengubah suara dan wajah seseorang untuk mengatakan hal-hal yang menyinggung atau seksual, sering kali tanpa sepengetahuan atau persetujuan korban. Masalah ini menjadi sangat penting karena mayoritas korban tidak memiliki akses terhadap alat pendeteksi *deepfake* atau dukungan teknologi untuk membuktikan bahwa konten tersebut palsu. Selain itu, banyak di antara mereka juga kesulitan mendapatkan pendampingan hukum atau perlindungan yang memadai, baik karena keterbatasan pengetahuan hukum, stigma sosial, maupun kurangnya dukungan institusional. Misalnya, perempuan seringkali menjadi subjek utama dalam film-film seksual yang telah diubah dengan teknologi ini. Nama buruk bukan satu-satunya dampak sosial dan mental. Hal ini juga dapat menyebabkan penyakit mental seperti gangguan stres pascatrauma (PTSD). (Dani, R. A. A. (2024).

Dalam konteks politik, disinformasi berbasis *deepfake* menimbulkan ancaman serius terhadap integritas demokrasi. Video manipulatif yang menargetkan politisi atau institusi publik dapat menggiring opini masyarakat dengan cara yang sulit dideteksi, memicu ketidakstabilan politik, dan bahkan mengubah hasil pemilu. Sebagai contoh, video *deepfake* yang menunjukkan seorang tokoh publik mengucapkan pernyataan yang kontroversial telah digunakan untuk merusak reputasi lawan politik atau menggiring narasi palsu. (Fadillah, N. M. F., & Setiawan, H., 2020)

Selain dampak sosial dan politik, *deepfake* juga membawa dimensi baru dalam kejahatan siber, terutama dalam bentuk penipuan finansial. Teknologi *deepfake* memungkinkan pelaku untuk meniru suara atau wajah seseorang dengan tingkat akurasi tinggi, sehingga dapat digunakan untuk menipu individu atau Perusahaan. Selain itu, kurangnya kepercayaan terhadap informasi digital semakin parah seiring menyebarnya konten *deepfake* di media sosial. Banyak pengguna media sosial kesulitan membedakan konten asli dan palsu, sehingga mengurangi kepercayaan terhadap media daring. Keadaan ini diperburuk oleh algoritma platform yang sering kali memprioritaskan konten sensasional, termasuk *deepfake,* karena potensi viralnya yang tinggi. Lebih jauh, *deepfake* juga memiliki dampak psikologis yang signifikan. Tidak hanya pada individu yang menjadi korban langsung, tetapi juga pada masyarakat secara keseluruhan yang terpapar disinformasi secara terus-menerus. (Kurniawan, A. A., & Mustikasari, M. (2020).

Deepfake juga dapat dijelaskan dalam beberapa pandangan, antara lain:

a) Penggunaan deepfake perspektif KHUP

Fenomena *deepfake* konten visual atau audio yang telah dipalsu dengan menggunakan kecerdasan buatan menimbulkan tantangan serius dalam sistem hukum Indonesia, terutama karena teknologi ini bisa dipakai untuk membentuk opini publik,

menjelekkan nama baik, atau menyebarkan konten pornografi tanpa izin. Regulasi saat ini memang tidak secara eksplisit menyebut istilah "*deepfake",* namun sejumlah pasal dalam KUHP menawarkan landasan hukum yang cukup untuk menjerat pelakunya. Di dalam KUHP *deepfake* dapat dipidana berdasarkan Pasal 407, yang mengancam pidana penjara antara 6 bulan hingga 10 tahun dan denda hingga Rp 2 miliar jika seseorang memproduksi atau menyebarluaskan konten pencemaran nama baik berbasis AI Sementara itu, *deepfake* yang merusak reputasi seseorang terutama yang disebarkan secara elektronik dapat dikategorikan sebagai pencemaran nama baik atau penghinaan, sehingga terancam pidana sesuai Pasal 433, 434, 436, dan 441 KUHP. Pasal-pasal tersebut menggantikan sebagian ketentuan UU ITE sehingga memberikan payung hukum yang lebih khusus dalam menjawab kejahatan digital modern. (Meliana, Y. (2025).

b) Penggunaan *deepfake* perspektif UU ITE

Penggunaan teknologi *deepfake* dalam perspektif UU ITE dipandang sebagai salah satu bentuk pemanfaatan teknologi informasi yang dapat menimbulkan konsekuensi hukum, terutama ketika digunakan untuk tujuan yang melanggar hukum atau merugikan pihak lain. UU ITE, khususnya Pasal 27 ayat (1) dan ayat (3), melarang distribusi, transmisi, dan/atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan melanggar kesusilaan atau pencemaran nama baik. Apabila *deepfake* digunakan untuk menciptakan konten pornografi tanpa persetujuan pihak yang bersangkutan, maka perbuatan tersebut dapat digolongkan sebagai pelanggaran terhadap ketentuan ini, yang diancam dengan pidana penjara hingga enam tahun dan/atau denda paling banyak satu miliar rupiah. (Sijabat, S. A. U., & Lukitasari, D. (2024).

Selain itu, *deepfake* yang dipakai untuk memanipulasi wajah atau suara seseorang dalam rangka menyebarkan informasi palsu dapat dikaitkan dengan Pasal 28 ayat (1) dan ayat (2) UU ITE, yang mengatur larangan penyebaran berita bohong dan informasi yang menimbulkan kebencian atau permusuhan berdasarkan SARA. Pasal-pasal ini dapat dikenakan jika penggunaan *deepfake* mengarah pada penipuan publik, fitnah, atau provokasi.

c) Penggunaan *deepfake* perspektif UU Perlindangan data pribadi

Teknologi *deepfake*, yang memungkinkan pembuatan konten visual atau audio realistis tapi sepenuhnya direkayasa secara digital, menimbulkan tantangan baru dalam ranah perlindungan data pribadi. Meskipun UU PDP belum menyebut istilah "*deepfake"* secara eksplisit, beberapa ketentuan dalam undang-undang ini tetap relevan, terutama menyangkut data pribadi yang digunakan tanpa izin. Pasal 4 UU PDP menetapkan bahwa "setiap orang berhak mendapatkan perlindungan atas data pribadinya. Dalam konteks *deepfake,* yang sering kali memanfaatkan gambar wajah atau suara seseorang tanpa persetujuan termasuk kategori data *biometric* ketentuan ini menjadi sangat penting sebagai dasar hukum untuk menjerat pelaku penyalahgunaan.

Pasal 9 UU PDP menekankan bahwa pengumpulan maupun penggunaan data pribadi hanya sah dilakukan apabila telah mendapat persetujuan yang sah dari pemilik data. Jika data tersebut digunakan untuk membuat konten *deepfake* tanpa izin, hal itu jelas melanggar ketentuan ini. UU PDP juga telah menetapkan sanksi yang tegas bagi pelanggaran seperti pemalsuan data pribadi. Pelanggaran ini diancam dengan pidana penjara maksimal 6 tahun dan/atau denda hingga Rp 6 miliar sebagaimana tercantum dalam Pasal 68 UU PDP. (Sijabat, S. A. U., & Lukitasari, D. (2024).

Tantangan sekarang adalah masih sulit untuk mendeteksi *deepfake* dengan akurasi tinggi. Terdapat aplikasi khusus untuk melakukan pengecekan *deepfake,* namun yang disayangkan belum ada aplikasi yang bisa melakukan pengecekan dengan tingkat keakurasian 100%. Sehingga hal ini membuat *deepfake* masih berperan kuat sebagai media penyebaran misinformasi. Aplikasi *deepfake* terkait konten politik bermuatan negatif merupakan

penyalahgunaan teknologi AI yang dijadikan sebagai alat oleh seseorang untuk mencemarkan nama baik seseorang. (Mahardika, M. I. (2025).

Oleh karena itu, dalam hal ini menekankan pentingnya regulasi adaptif yang mampu mengakomodasi kompleksitas teknologi *deepfake.* Regulasi seperti *Artificial Intelligence Act* di Uni Eropa dapat menjadi contoh bagaimana pendekatan hukum dapat digunakan untuk mengontrol penggunaan teknologi baru tanpa membatasi inovasi. Selain itu, pengembangan teknologi deteksi yang lebih maju, literasi digital yang komprehensif, dan kerja sama internasional menjadi elemen penting dalam upaya global untuk mengurangi dampak negatif teknologi ini dan menjaga kepercayaan masyarakat terhadap informasi digital.

Bentuk Tanggung Jawab Hukum Terhadap Korban Penyalahgunaan *Artificial Intelligence* Terkhususnya Teknik Deepfake Dalam Kejahatan Pencemaran Nama Baik

Seiring berkembangnya teknologi Artificial Intelligence (AI), banyak aspek kehidupan telah ditingkatkan, seperti bisnis, layanan kesehatan, pendidikan, dan hiburan. Namun, seiring dengan manfaat tersebut, muncul pula potensi penyalahgunaan teknologi AI, salah satunya dalam bentuk *deepfake* yaitu teknik manipulasi visual atau audio menggunakan algoritma deep learning yang menghasilkan konten palsu namun tampak nyata. Dengan *deepfake*, guna alasan tertentu, seseorang bisa berbohong kepada publik dan mengatakan bahwa seseorang mengatakan atau melakukan sesuatu yang tidak dilakukannya. Orang yang menggunakan deepfake untuk mencemarkan nama baik atau citra seseorang melanggar hukum.

Dasar negara dalam hal ini telah memberikan perlindungan terhadap individu itu sendiri, keluarga dan harta benda yang dimiliki. Hak asasi manusia dilanggar ketika seseorang mengatakan hal-hal buruk tentang orang lain, terutama hak atas kehormatan dan nama baik. Jika seseorang difitnah melalui konten deepfake, negara diwajibkan oleh Konstitusi untuk melindungi hak-hak mereka melalui perangkat hukum pidana dan perdata yang sesuai. (Rahman, A. U. N. F., Syariffudin, S., & Bari, F. (2025).

Dengan menyatukan teknologi, data, dan kebebasan manusia, kita dapat mengubah cara kerja masyarakat. UU ITE disusun oleh negara dan pemerintah Indonesia untuk menangani kejahatan yang berkaitan dengan penggunaan teknologi. Hal ini karena kejahatan dalam bidang hukum ini pasti terjadi. Menurut UU ITE, informasi pribadi dan hak privasi setiap orang dilindungi. Selain itu, undang-undang ini menetapkan aturan untuk teknologi dan informasi dan memberikan landasan hukum bagi banyak hal digital. (Rahman, A. U. N. F., Syariffudin, S., & Bari, F. (2025).

Tidak ada undang-undang yang secara langsung mengatur bagaimana orang yang mencemarkan nama baik orang lain menggunakan aplikasi *deepfake* harus dihukum dan bagaimana mereka harus dilindungi. Namun, konstitusi telah mengubah aturan untuk menangani masalah seperti fitnah, pencurian identitas, dan pemalsuan menggunakan aplikasi deepfake. Berikut bagian-bagian hukum dan peraturan Indonesia yang mengatur *deepfake*:

a) UU No.1 Tahun 2024 mengenai Perubahan ke 2 atas UU No.11 Tahun 2008 tentang ITE

Pasal 27 memberikan suatu penegasan yakni jika bagi individu yang secara sadar dan tanpa izin menyebarluaskan, mempertontonkan, mendistribusikan, mengirimkan, atau memberikan akses pada suatu Informasi Elektronik maupun Dokumen Elektroniik yang terdapat suatu pidana terhadap norma kesusilaan kepada khalayak umum, dapat dinilai sebagai pelanggaran hukum yang berlaku saat ini.

Tindakan *deepfake* relevan dengan ayat (3), yang telah disesuaikan dengan Pasal 27a yakni: Jika seseorang dengan sengaja melakukan sesuatu yang merugikan kehormatan atau citra orang lain, seperti membuat tuduhan, dan bertujuan agar tuduhan tersebut diketahui oleh khalayak luas, serta disampaikan melalui media berbentuk Data digital dengan menggunakan Sistem Elektronik, tindakan ini menyalahi Hak fundamental yang terdapat dalam beberapa aturan. Hal ini dijelaskan dalam Pasal 45 ayat (1) UU ITE, yang membahas

hukuman yang akan dihadapi seseorang jika melanggar aturan ini. Ada potensi hukuman penjara 6 tahun dan/atau denda 1 miliiar. (Khalishah, K., Wulandari, L., & Ardiansyah, R. (2024).

b) UU No.27 2022 mengenai Perlindungan Data Pribadi

Pasal 66 dalam undang-undang ini memuat ketentuan tentang: Setiap individu tidak diperbolehkan untuk menciptakan atau memanipulasi data pribadi secara tidak benar bertujuan memperoleh keuntungan pribadi maupun untuk memberikan keuntungan kepada pihak lain, tindakan ini berpotensi merugikan orang lain. Pasal ini bermanfaat karena teknologi deepfake dapat mengubah gambar atau video dengan wajah orang lain, karena wajah ialah data biologis yang unik. Pasal 66 Undang-Undang ini menyatakan orang yang melanggarnya dapat dihukum hingga enam tahun penjara atau denda enam miliar rupiah. (Khalishah, K., Wulandari, L., & Ardiansyah, R. (2024).

Dari aspek hukum pidana, aturan ini mencakup pencemaran nama baik. Telah dijabarkan pada Pasal 310 KUHP menyatakan segala bentuk tindakan yang sengaja menyudutkan atau merendahkan martabat seseorang melalui tuduhan tertentu tergolong sebagai pelanggaran hukum, dan dengan sengaja bermaksud agar tuduhan tersebut diketahui oleh masyarakat luas, dapat dikenai sanksi pidana atas perbuatan pencemaran yakni kurungan selama 9 bulan serta denda sebesar Rp4.500,-. (Permana, I. P. A., Arjaya, I. M., & Karma, N. M. S. (2021).

Pelaku pencemaran dalam hal ini haruslah wajib tunduk pada UU ITE, yakni UU No.11 Tahun 2008 jo. UU No.19 Tahun 2016. Pasal 27 Bagian 3 UU ITE menyebutkan, setiap orang yang dengan sengaja dan tanpa izin mengirimkan, membagikan, atau memberikan akses pada informasi atau data digital yang terdapat unsur menyinggung atau memfitnah, dapat dianggap melanggar hak reputasi yang dilindungi undang-undang.

Dengan demikian, setiap orang yang membuat dan membagikan video *deepfake* yang berisi fitnah dapat dikenai pasal pidana berdasar Pasal 27 dan 24 dalam hal ini juga memberikan suatu penjelasan mengenai individu yang terbukti melakukan perbuatan yang terdapat dalam pasal tersebut maka bisa dijatuhi sanksi berupa hukuman penjara dengan masa maksimal empat tahun dan/atau dikenakan denda paling banyak sebesar 750 juta.

Selain ancaman pidana, korban *deepfake* juga dapat menempuh jalur perdata untuk mendapatkan ganti rugi atas kerugian immaterial yang diderita, baik berupa terganggunya psikologis, hilangnya kepercayaan publik, maupun rusaknya reputasi profesional. Dasar hukum perdata ini merujuk pada Pasal 1365 KUHPer menyatakan jika seseorang secara melawan hukum dan merugikan orang lain, orang tersebut bertanggung jawab untuk mengganti kerugiannya.

Ketika seseorang melakukan tindakan ilegal seperti *deepfake*, ia melanggar hukum dengan tidak menghormati privasi dan kehormatan orang lain. Pembuatan dan penyebaran konten *deepfake* yang menyerang nama baik seseorang jelas melanggar hukum, sehingga korban berhak untuk menuntut ganti rugi di pengadilan perdata. Dalam konteks pertanggungjawaban pelaku, hukum pidana mengenal asas subjektif dan objektif. Secara subjektif, pelaku *deepfake* dapat dinyatakan bertanggung jawab secara pidana apabila terbukti bahwa ia secara sadar dan sengaja menciptakan atau menyebarkan konten yang merusak nama baik orang lain. Secara objektif, pertanggungjawaban tersebut dilihat dari akibat hukum yang ditimbulkan, yakni rusaknya reputasi korban. Pertanggungjawaban ini diperkuat jika pelaku mengetahui konten tersebut adalah palsu namun tetap menyebarkannya, atau bahkan menciptakannya sendiri. (Novyanti, H., & Astuti, P. (2021).

Beberapa kasus di luar negeri, teknik *deepfak*e juga sudah dipakai guna menyebarkan konten palsu dengan wajah figur publik. Hal ini jika terjadi di Indonesia, juga bisa dihukum melalui Pasal 27 ayat (1) UU ITE mengenai isi yang melanggar standar moral dan Pasal 29 tentang ancaman melalui media elektronik. Hal ini menunjukkan bahwa perangkat hukum

Indonesia, meskipun belum secara spesifik menyebutkan teknologi *deepfake,* namun cukup fleksibel dalam mengakomodasi tindakan semacam itu melalui interpretasi terhadap istilah "muatan elektronik". (Novyanti, H., & Astuti, P. (2021).

Tanggung jawab hukum terhadap korban *deepfake* juga tidak hanya terbatas pada pelaku utama, tetapi dapat diperluas kepada pihak-pihak yang turut membantu penyebaran konten, misalnya media sosial atau platform digital yang lalai dalam menyaring dan menghapus konten bermuatan pencemaran nama baik. Perusahaan platform digital dapat dikenai tanggung jawab hukum melalui prinsip tanggung jawab hukum korporasi sebagaimana diatur dalam Pasal 52 UU ITE. Dalam praktiknya, bentuk tanggung jawab ini akan terkait dengan keharusan mereka untuk menyediakan sistem deteksi dini, penghapusan konten berbahaya, dan kerja sama aktif dengan aparat penegak hukum. (Purnomo, H. (2020).

Meskipun demikian, dalam konteks pembuktian, perkara pencemaran nama baik melalui *deepfake* memiliki tantangan tersendiri. Keaslian dan manipulasi digital harus diuji melalui keahlian forensik digital, sehingga memerlukan kerja sama dengan ahli teknologi informasi. Korban juga harus mampu menunjukkan bahwa video tersebut palsu dan bahwa penyebarannya menyebabkan kerugian yang signifikan. Hal ini seringkali membutuhkan biaya dan proses yang tidak singkat, terutama apabila pelaku tidak berada dalam yurisdiksi Indonesia. Untuk itu, negara juga perlu membentuk regulasi yang secara khusus mengatur penggunaan teknologi *deepfake* dalam ranah hukum. (Purnomo, H. (2020). Aturan ini harusnya menjadi paying hukum terhadap pelanggaran yang berakitan dengan deepfake dan setiap perbuatan yang juga berkaitan dengan elektronik. Pasal 65(1) UU PDP menyatakan pelaku dipidana dengan pidana kurungan dengan kurun waktu 5 tahun serta denda 5 sebanyak miliiar jika menggunakan informasi pribadi orang lain tanpa izin dan dengan sengaja. Ini karena tindakan orang tersebut dapat menimbulkan kerugian.

Dengan demikian, penggunaan gambar, suara, atau identitas digital seseorang dalam konten *deepfake* yang dibuat tanpa izin dapat dikategorikan sebagai pelanggaran terhadap perlindungan data pribadi, dan pelakunya dapat dimintai pertanggungjawaban secara pidana.

Bentuk tanggung jawab terhadap kasus ini tidak hanya pada ranah pidana, namun pada kompensasi yang harus diterima oleh korban, Apa pun tahap persidangannya atau apa pun keputusannya, kompensasi adalah ketika korban meminta uang dari publik atau pemerintah. Tujuan dari kompensasi guna meningkatkan kesejahteraan masyarakat. Sebagai pemerintah yang bertanggung jawab, pemerintah berkewajiban melindungi seluruh rakyatnya. Restitusi ialah ganti rugi yang dibayarkan pelaku berdasarkan putusan pengadilan, sedangkan kompensasi merupakan ganti rugi dari negara jika pelaku tidak mampu membayar denda tersebut. (Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024).

Tanggung jawab hukum pada korban penyalahgunaan AI dalam bentuk teknik deepfake mencakup dimensi pidana, perdata, serta administrasi perlindungan data pribadi. Instrumen hukum yang berlaku saat ini seperti KUHP, UU ITE, KUH Perdata, dan UU PDP telah memberikan dasar yang cukup untuk menjerat pelaku kejahatan dan memberikan perlindungan hukum kepada korban, meskipun regulasi yang lebih spesifik mengenai deepfake dan teknologi manipulasi berbasis AI masih sangat diperlukan. Memberikan perlindungan hukum kepada korban tidak terbatas pada pemidanaan pelaku, tetapi juga memastikan bahwa korban mendapatkan pemulihan nama baik, hak atas rehabilitasi sosial, dan keadilan atas kerugian yang diderita akibat kejahatan digital berbasis teknologi canggih seperti deepfake. Subekti, A. S., Pradana, N. A. S., Ardhira, A. Y., & Zulfikar, M. T. I. (2021).

Analisis Kasus *Deepfake* Terkait Pencemaran Nama Baik

Menurut hasil survei oleh *Deeptreace* yang diselenggarkaan tahun 2019, sebanyak 96% dari video deepfake yang beredar di internet mengandung unsur pornografi. Contoh kasus yang menjadi sorotan di Indonesia yakni dugaan video asusila yang menampilkan sosok mirip

dengan artis Nagita Slavina. Kasus ini dilaporkan oleh Pitra Romadoni Nasution dan tercatat dalam laporan polisi di Polres Metro Jakarta Pusat dengan nomor LP/B/100.1/2002/SPKT/RESORT JAKPUS/PMJ tertanggal 13 Januari 2022. Video berdurasi 61 detik tersebut mulai beredar di dunia maya sejak Januari 2022. (Tim detikcom, 22 Juli 2025)

Dalam laporannya, pelapor menuntut pemilik akun penyebar video berdasarkan ketentuan Pasal 6 dan Pasal 8 UU No.4 Tahun 2008 mengenai Pornografi, serta Pasal 27 ayat (1) UU No.19 Tahun 2016 tentang (ITE). Terkait laporan ini, Tim Siber dari Polda Metro Jaya melakukan investigasi dan menemukan bahwa video tersebut merupakan hasil rekayasa teknologi *deepfake.*

Kongres Pemuda Indonesia (KPI) juga turut melaporkan video ini karena dinilai telah meresahkan masyarakat. Namun, proses penanganan menjadi sulit karena pelapor tidak mengetahui asal mula video maupun siapa pembuatnya. Wisnu, anggota Tim Siber Polda Metro Jaya, menyatakan bahwa pihaknya masih perlu melakukan klarifikasi lebih lanjut kepada pelapor yang hanya menyerahkan tangkapan layar dari video tersebut, sehingga belum bisa dipastikan bentuk video yang dimaksud. Laporan tersebut meminta aparat kepolisian untuk menyelidiki dan mengusut penyebaran video tersebut secara menyeluruh. Namun demikian, video ini telah viral di berbagai platform media sosial, sehingga pelacakan terhadap sumber awal menjadi sangat sulit dilakukan. Jumlah akun yang melakukan unggahan ulang terlalu banyak, sehingga tidak memungkinkan untuk menindak semuanya. (Faqih dan Soerjati Priowirjanto, 2022)

Kasus video *deepfake* yang menyeret nama Nagita Slavina menunjukkan adanya tantangan serius dalam proses pembuktian hukum. Ketika sebuah konten telah tersebar luas dan diunggah oleh banyak pihak, akan sangat sulit melacak siapa yang pertama kali menyebarkannya. Apalagi, identitas pengguna media sosial dapat dengan mudah dipalsukan menggunakan akun dan email fiktif. (Hidayati, N. (2024).

Dalam hukum pidana Indonesia, penggunaan *deepfake* yang berisi muatan penghinaan atau pencemaran nama baik diatur dalam Pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (*UU ITE*) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik, dapat dipidana penjara paling lama empat tahun dan/atau denda paling banyak Rp750.000.000,00. (Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025). Selain itu, jika *deepfake* tersebut bermuatan pornografi, pelaku juga dapat dijerat dengan Pasal 29 juncto Pasal 4 ayat (1) huruf d Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, yang mengancam pelaku dengan pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp6.000.000.000,00. (Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025).

Dari sudut pandang pertanggungjawaban pidana, perbuatan ini memenuhi unsur *actus reus* berupa tindakan menciptakan atau menyebarkan *deepfake* yang mengandung muatan pencemaran nama baik, serta unsur *mens rea* berupa kesengajaan (*dolus*) dalam membuat atau menyebarkan konten tersebut untuk menyerang kehormatan atau reputasi korban. Teori *mens rea* menekankan bahwa pertanggungjawaban pidana baru dapat dibebankan jika pelaku mengetahui dan menghendaki akibat dari perbuatannya. Dengan demikian, pelaku yang secara sadar memproduksi dan mendistribusikan *deepfake* yang merusak reputasi dapat dimintai pertanggungjawaban penuh. (Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025).

Selain itu, apabila pembuatan atau penyebaran *deepfake* dilakukan oleh lebih dari satu orang dalam bentuk kerja sama atau kolaborasi (*organized crime*), maka Pasal 55 dan Pasal 56 Kitab Undang-Undang Hukum Pidana (*KUHP*) mengenai penyertaan dapat diterapkan. Hal ini berarti tidak hanya pembuat konten, tetapi juga pihak yang memerintahkan atau turut membantu penyebaran dapat dimintai pertanggungjawaban pidana.

Sebagaimana telah dijelaskan sebelumnya, teknologi *deepfakes* memungkinkan seseorang dengan mudah menempelkan wajah individu lain ke dalam video tertentu hanya dengan mengumpulkan sejumlah besar foto guna dianalisis dan diproses oleh algoritma. Kemudahan inilah yang membuka peluang bagi pihak-pihak dengan niat jahat untuk menciptakan konten video bermuatan pornografi. Penyalahgunaan teknologi ini dalam pembuatan video pornografi yang menyertakan wajah orang lain tanpa izin, jika ditinjau dari ketentuan dalam Undang-Undang Pornografi, jelas merupakan tindakan yang dilarang. Hal ini dikarenakan video tersebut dibuat tanpa sepengetahuan maupun persetujuan dari individu yang wajahnya digunakan, sesuai Pasal 9 UU Pornografi. Pasal 8 UU yang sama menyatakan seseorang dilarang menggunakan dirinya sebagai objek atau figur dalam materi pornografi, baik dengan sengaja maupun dengan izinnya. (Kusuma, L. P. Y. R., Dewi, A. A. S. L., & Suryani, L. P. (2022).

Pasal 9 UU Pornografi menyatakan setiap orang yang menambahkan wajah orang lain ke dalam video pornografi tanpa izin dipidana karena telah melakukan kedua hal yang termasuk dalam tindak pidana: (1) membuat video tersebut; dan (2) menggunakan orang lain sebagai model dalam konten pornografi. Jika melanggar Pasal 35 dan Pasal 9 UU Pornografi, pelaku dipenjara hingga 12 tahun atau membayar denda hingga 6 miliiar. (Novera, O. (2024).

Pasal 27 ayat (1) UU ITE menyatakan perbuatan tersebut adalah perbuatan melawan hukum. Pasal tersebut menyatakan bahwa siapa pun yang dengan sengaja menyebarkan, mengirim, atau membuat bisa diaksesnya informasi atau data digital yang mengandung muatan tertentu, dilarang oleh hukum yang salah secara moral. Dalam hal ini, jelas bahwa materi video seksual ialah bentuk pelanggaran moral.

Selain itu, Pasal 27 ayat (3) UU ITE juga menyatakan setiap orang dilarang secara sadar membagikan atau menyediakan data digital yang dalam hal ini mengandung kebohongan atau penghinaan terhadap orang lain tanpa izin. Dengan ini, penulis bermaksud membuat dan membagikan video seksual sama dengan menghina kehormatan atau harga diri seseorang, yang ialah perbuatan melawan hukum menurut Pasal 310 ayat (1) dan (2) KUHP. Menyebarkan film porno yang menampilkan orang awam seperti Nagita Slavina merupakan contoh nyata pencemaran nama baik. (Wahyudi, R. (2024).

Orang yang melanggar aturan dari yang tersebut diatas maka dalam hal ini bisa dikenai hukuman kurungan hingga 6 tahun ataupun pembayaran denda sebanyak 1 miliiar. Selanjutnya, Pasal 38 ayat (1) UU ITE memberikan ruang bagi setiap orang yang dirugikan akibat penyelenggaraan sistem elektronik atau penggunaan teknologi informasi untuk mengajukan gugatan. Oleh karena itu, korban yang dirugikan secara pribadi akibat penyebaran konten deepfake tersebut juga berhak mengajukan tuntutan ganti rugi, sehingga pelaku tidak hanya dapat dimintai pertanggungjawaban secara pidana, tetapi juga secara perdata.

KESIMPULAN

Penyalahgunaan teknologi *Artificial Intelligence,* khususnya *deepfake,* telah melahirkan bentuk kejahatan digital baru yang meresahkan, terutama terkait pencemaran nama baik melalui manipulasi visual atau audio. *Deepfake* kerap digunakan untuk membuat konten palsu yang merusak reputasi seseorang tanpa keterlibatan langsung korban, dengan sebagian besar disalahgunakan untuk pornografi atau pelecehan digital, berdampak serius secara psikologis dan sosial. Dalam konteks hukum Indonesia, pelaku penyebaran konten *deepfake* yang mengandung unsur pencemaran nama baik dapat dijerat melalui Pasal 27 ayat (1) dan (3) jo. Pasal 45 UU ITE, Pasal 310 KUHP, Pasal 9 UU Pornografi, serta Pasal 66 UU PDP. Selain sanksi pidana, korban juga dapat mengajukan gugatan perdata melalui Pasal 1365 KUH Perdata. Pertanggungjawaban juga bisa diperluas pada pihak penyebar maupun platform digital yang lalai. Kasus seperti yang dialami Nagita Slavina menunjukkan tantangan penegakan hukum, terutama dalam pelacakan pelaku dan pembuktian. Karena itu, diperlukan pembaruan

regulasi, peningkatan literasi digital, dan kolaborasi antara pemerintah, aparat, ahli teknologi, dan platform digital untuk melindungi korban secara efektif.

Pemerintah perlu segera menetapkan aturan yang jelas mengenai pemakaian dan penyalahgunaan teknologi kecerdasan buatan, seperti *deepfake,* secara menyeluruh dalam aspek pidana, perdata, dan perlindungan data pribadi agar selaras dengan perkembangan teknologi yang pesat. Di samping itu, peningkatan literasi digital bagi masyarakat luas menjadi sangat penting agar individu mampu mengenali bahaya dari teknologi manipulatif seperti *deepfake* dan tidak ikut serta dalam penyebaran konten yang merugikan orang lain. Tak kalah penting, platform media sosial dan penyedia layanan digital juga dituntut untuk berperan aktif dalam menyaring, menghapus, serta melaporkan konten *deepfake* yang merugikan, sekaligus menyediakan mekanisme pelaporan yang mudah dijangkau oleh pengguna demi menjamin perlindungan yang lebih efektif.

REFERENSI

Arvitto, Rafi, (2025), Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP, *Jurnal Ilmiah Hukum dan Hak Asasi Manusia,* 4 (73)

Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut Hukum positif Indonesia. *Dinamika*, *30*(1), 9675-9691

Basah, D. A. Y., Wijaya, A., & Januardy, I. (2025). Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial. *Innovative: Journal Of Social Science Research*, *5*(4), 386-398.

Dani, R. A. A. (2024). Pencemaran Nama Baik Melalui Media Sosial Berdasarkan Putusan Nomor 26/PID. SUS/2022/PT SBY. *Jurnal Ilmiah Wahana Pendidikan*, *10*(10), 720-742.

Faathurrahman, M. F., & Priowirjanto, E. S. (2022). Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia. *Jurnal Indonesia Sosial Teknologi,* 3(11), 1156-1168

Hidayati, N. (2024). Analisis Hukum Tentang Aspek Pembuktian Terhadap Perkara Pencemaran Nama Baik Melalui Media Sosial. *Jurnal Lawnesia (Jurnal Hukum Negara Indonesia)*, *3*(2), 494-506.

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

Kusuma, L. P. Y. R., Dewi, A. A. S. L., & Suryani, L. P. (2022). Sanksi Pidana Pelaku Pencemaran Nama Baik Melalui Media Sosial. *Jurnal Konstruksi Hukum*, *3*(2), 333-337.

Kasita, I. D. (2022). Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KBGO) Di Era Pandemi Covid-19. *Jurnal Wanita dan Keluarga*, 3(1), 16-26

Khalishah, K., Wulandari, L., & Ardiansyah, R. (2024). Perlindungan Hukum Terhadap Perempuan Korban Balas Dendam Pornografi Dengan Mempergunakan Aplikasi "Deepfake" Sebagai Kekerasan Berbasis Gender Online. *Parhesia*, *2*(2), 1-14

Martinelli, I., Yohana, Y., Venessa, C., & Hiumawan, E. J. (2023). Urgensi Pengaturan dan Perlindungan Rights of Privacy terhadap Artificial Intelligence dalam Pandangan Hukum sebagai Social Engineering. *Jurnal Tana Mana*, *4*(2), 157-166

Mahardika, M. I. (2025). TINJAUAN YURIDIS TERHADAP PELAKU DEEPFAKE PORN SEBAGAI KEKERASAN GENDER BERBASIS ONLINE MENURUT UU PORNOGRAFI. *LEX PRIVATUM*, *14*(5)

Marzuki, P. M. (2021). *Penelitian Hukum*. Jakarta: Kencana

Meliana, Y. (2025). Urgensi Formulasi Perlindungan Hukum dan Kepastian Pidana terhadap Pengaturan Tindak Pidana Deepfake dalam Sistem Hukum Pidana Nasional. *Jurnal Hukum Lex Generalis*, *6*(7).

Mongkau, N. H., Bawole, H. Y. A., & Musa, A. (2025). Penegakkan Hukum Terhadap Penyalhgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Ke Dalam Gambar Atau Video Porno. *LEX ADMINISTRATUM*, *13*(2

Nugroho, T. A., Amarco, A. K., & Yasin, M. (2023). Perkembangan Industri 5.0 Terhadap. Perekonomian Indonesia. *Manajemen Kreatif Jurnal (MAKREJU),* 1(3), 95-106

Nurlatifah, A., Thalib, H., & Khalid, H. (2021). Pertanggungjawaban Pidana Terhadap Pelaku Pencemaran Nama Baik Melalui Media Sosial: Studi Putusan Nomor 1481/Pid. Sus/2020/PN-Mks. *Journal of Lex Generalis (JLG)*, *2*(8), 2244-2252

Novyanti, H., & Astuti, P. (2021). Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana. *Novum: Jurnal Hukum*, 31-40

Novera, O. (2024). Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (deepfake) dalam penyebaran konten pornografi melalui akun media sosial. *El-Faqih: Jurnal Pemikiran dan Hukum Islam*, *10*(2), 460-474.

Permana, I. P. A., Arjaya, I. M., & Karma, N. M. S. (2021). Peranan Alat Bukti Elektronik dalam Tindak Pidana Pencemaran Nama Baik. *Jurnal Interpretasi Hukum*, *2*(2), 422-428.

Prayoga, H., & Tuasikal, H. (2025). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. *Abdurrauf Law and Sharia*, *2*(1), 22-38.

Purnomo, H. (2020). Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Melalui Media Berdasarkan Konsep Hukum Pidana. *Soumatera Law Review*, *3*(2), 119-134.

Rahman, A. U. N. F., Syariffudin, S., & Bari, F. (2025). Perlindungan Hukum terhadap Korban Penyalahgunaan Teknik Deepfake. *Perspektif Administrasi Publik dan hukum*, *2*(1), 247-255

Ramadhani, R. A., Rahman, S., & Bima, M. R. (2024). Efektivitas Hukum Terhadap Pencemaran Nama Baik Melalui Melalui Penggunaan Meme Internet Media Sosial. *Journal of Lex Philosophy (JLP)*, *5*(2), 380-390.

Situmeang, B. S., Silitonga, I. Y., Silaen, R. F., Siringoringo, T. H., & Sipayung, E. E. (2024). Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deep Fake Pada Selebritas di Twitter. *Device*, *14*(1), 80-91

Sijabat, S. A. U., & Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik. *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *13*(2), 179-194

Suryokencono, P., & Isyraq, R. F. (2024). Perlindungan Hukum Berupa Pemulihan Nama Baik Terhadap Korban Tindak Pencemaran Nama Baik Melalui Situs Deepfake. *National Multidisciplinary Sciences*, *3*(4), 587-596.

Subekti, A. S., Pradana, N. A. S., Ardhira, A. Y., & Zulfikar, M. T. I. (2021). Tindak Pidana Pencemaran Nama Baik Melalui Facebook Menurut KUHP dan Undang-Undang Nomor 11 Tahun 2008 Tentang ITE. *Jurnal Hukum & Pembangunan*, *50*(3), 738-757.

Utawi, E. i., & Ruhaeni, N. (2023). Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial. Bandung *Conference Series: Law Studies*, 3(1), 365-372

Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis hukum terhadap upaya pencegahan kasus deepfake porn dan pendidikan kesadaran publik di lingkungan digital. *Jurnal Pendidikan Tambusai*, *7*(3), 26179-26188.

Wahyudi, R. (2024). Tindakan Pencemaran Nama Baik Melalui Media Sosial Dalam Perspektif Hukum Pidana. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 17-25.