



KAJIAN HUKUM TERHADAP PENGGUNAAN ARTIFICIAL INTELLIGENCE (AI) YANG BERAKIBAT MENYERANG KEHORMATAN

Nadiyah¹, Ronny Winarno², Wiwin Ariesta³

^{1,2,3}Universitas Merdeka Pasuruan, Indonesia

E-mail: nnadiyah25@gmail.com¹, ronny@unmerpas.ac.id², wiwinariesta@unmerpas.ac.id³

Received 18-05-2025 | Revised form 20-06-2025 | Accepted 21-07-2025

Abstract

The development of digital technology, particularly Artificial Intelligence, has provided various conveniences in human life, but it has also presented new legal challenges. One of these is the misuse of Artificial Intelligence, which has resulted in attacks on individual honor, such as through the creation of deepfake content. This study aims to analyze the criteria and processes for criminal acts that attack honor and examine criminal liability under Article 27A of Law of the Republic of Indonesia Number 1 of 2024. The research method used is normative juridical with a statutory approach and case studies. The results indicate that acts of attacking honor using Artificial Intelligence can be categorized as a crime if they meet the elements of intent, are disseminated to the public, and are in the form of electronic information. Article 27A of Law of the Republic of Indonesia Number 1 of 2024 provides a legal basis for prosecuting perpetrators, but does not explicitly regulate Artificial Intelligence as a tool or indirect perpetrator. This complicates the process of establishing evidence for law enforcement officials. Therefore, legal policies that are more adaptive to technological advances and concrete legal protection for victims of Artificial Intelligence abuse are needed.

Keywords: Artificial Intelligence, Honor, Deepfake, Article 27A of the ITE Law, Criminal Acts, Criminal Liability

Abstrak

Perkembangan teknologi digital, khususnya Artificial Intelligence, telah memberikan berbagai kemudahan dalam kehidupan manusia, namun juga menghadirkan tantangan hukum baru. Salah satunya adalah penyalahgunaan Artificial Intelligence yang berdampak pada serangan terhadap kehormatan individu, seperti melalui pembuatan konten deepfake. Penelitian ini bertujuan untuk menganalisis kriteria dan proses terjadinya tindak pidana yang menyerang kehormatan serta menelaah pertanggungjawaban pidana berdasarkan Pasal 27A Undang-Undang Republik Indonesia Nomor 1 Tahun 2024. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Hasil penelitian menunjukkan bahwa tindakan menyerang kehormatan dengan menggunakan Artificial Intelligence dapat dikategorikan sebagai tindak pidana apabila memenuhi unsur kesengajaan, disebarluaskan untuk diketahui umum, dan berbentuk informasi elektronik. Pasal 27A Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 memberikan dasar hukum untuk menjerat pelaku, namun belum mengatur secara eksplisit mengenai Artificial Intelligence sebagai alat atau pelaku tidak langsung. Hal ini menyulitkan aparat penegak hukum dalam proses pembuktian. Oleh karena itu, diperlukan kebijakan hukum yang lebih adaptif terhadap kemajuan teknologi serta perlindungan hukum yang konkret bagi korban penyalahgunaan Artificial Intelligence

Kata Kunci: Artificial Intelligence, Kehormatan, Deepfake, Pasal 27A UU ITE, Tindak Pidana, Pertanggungjawaban Pidana.

This is an open access article under the CC BY-NC-SA license.



PENDAHULUAN

Kemajuan teknologi yang pesat telah mengubah cara hidup masyarakat dari sistem konvensional menjadi digital, mempermudah berbagai aktivitas manusia, termasuk komunikasi, bisnis, hingga pemerintahan. Perkembangan teknologi informasi berdampak besar terhadap pola hidup masyarakat dan turut melahirkan tantangan baru dalam aspek hukum, salah satunya kejahatan siber (*cybercrime*). *Cybercrime* merupakan bentuk kejahatan yang melibatkan komputer sebagai alat maupun sasaran, yang kemudian mendorong urgensi pembentukan regulasi hukum baru (*ius constituendum*).¹

Salah satu hasil inovasi teknologi yang signifikan adalah kecerdasan buatan (*artificial intelligence/AI*), di mana Indonesia tercatat sebagai pengguna ketiga terbanyak secara global pada tahun 2023. Meskipun AI menawarkan banyak manfaat, penyalahgunaannya juga menimbulkan dampak serius, seperti penyerangan kehormatan individu melalui konten manipulatif, seperti deepfake. Kasus semacam ini telah menimbulkan keresahan publik karena dapat mencemarkan nama baik dan melanggar hak privasi.²

Dalam hukum Indonesia, penghinaan dan pencemaran nama baik diatur dalam Pasal 310 KUHP dan diperbarui melalui Pasal 27A UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Perubahan ini bertujuan menghindari multitafsir dan memberikan kepastian hukum dengan menekankan bahwa serangan kehormatan harus dilakukan secara sengaja melalui sistem elektronik agar diketahui umum. Namun demikian, regulasi yang ada belum mengatur secara khusus mengenai penyalahgunaan AI, sehingga menimbulkan celah hukum yang menyulitkan aparat dalam proses penyelidikan dan penegakan hukum.³

Fenomena penyebaran konten deepfake yang menyerang nama baik publik figur, seperti dalam kasus video palsu yang menampilkan Nagita Slavina, menunjukkan celah regulasi dan lemahnya perlindungan hukum atas penyalahgunaan AI. Konten semacam itu tidak hanya melanggar UU ITE, tetapi juga dapat dikenakan pasal dalam KUHP, UU Pornografi, maupun UU Perlindungan Data Pribadi, tergantung pada isi dan dampaknya.

¹ Ronny Winarno, Bambang Sudjito, Yudhia Ismail, 2020, *Pengantar Ilmu Hukum*, Malang: Intelegensia Media, hal 3

² Dikutip dari Databoks, *Indonesia Penyumbang Kunjungan Aplikasi AI Terbanyak ke-3 di Dunia*, dalam <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/a49ed3eb121983b/indonesia-penyumbang-kunjungan-ai-terbanyak-ke-3-di-dunia>, Diakses pada 31 Januari 2024, 13: 23 WIB.

³ Santosa, P. I. 2017. *Analisis Data dengan Machine Learning*. Yogyakarta: Andi Offset.

Kasus ini menjadi contoh konkret pentingnya regulasi yang komprehensif untuk menanggulangi kejahatan digital berbasis AI.⁴ Meskipun sudah ada laporan polisi terkait penyebaran video deepfake tersebut, proses hukum masih berjalan lambat dan belum menghasilkan kejelasan apakah kasus ini akan berlanjut ke pengadilan. Hal ini memperlihatkan kelemahan dalam sistem hukum dalam merespons kejahatan yang semakin canggih. Oleh karena itu, diperlukan pembaruan regulasi yang lebih spesifik mengenai AI serta penguatan kapasitas aparat penegak hukum agar mampu mengidentifikasi, menindak, dan memberikan perlindungan hukum yang maksimal terhadap korban kejahatan digital, khususnya dalam kasus yang menyangkut kehormatan dan integritas pribadi.

METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang bertumpu pada pengkajian terhadap norma-norma hukum tertulis yang relevan dengan permasalahan hukum yang dikaji, dalam hal ini berkaitan dengan penggunaan Artificial Intelligence (AI) yang berimplikasi menyerang kehormatan individu. Pendekatan ini dipilih karena objek yang diteliti berkaitan dengan ketentuan hukum positif, baik yang tertuang dalam undang-undang maupun dalam doktrin serta putusan pengadilan.⁵

Jenis data yang digunakan adalah data sekunder, yang mencakup bahan hukum primer, sekunder, dan tersier. Bahan hukum primer terdiri atas peraturan perundang-undangan seperti Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana (KUHP), serta Putusan Mahkamah Konstitusi terkait Pasal 27A. Bahan hukum sekunder mencakup literatur-literatur hukum, jurnal ilmiah, dan pendapat para ahli hukum yang relevan dengan topik. Sementara itu, bahan hukum tersier berupa kamus hukum dan ensiklopedia hukum yang digunakan untuk mendukung pemahaman konsep-konsep hukum.⁶

Teknik pengumpulan data dilakukan melalui studi kepustakaan, yaitu dengan mengakses dan mengumpulkan dokumen hukum, buku referensi, artikel ilmiah, dan sumber-sumber akademik lainnya yang relevan. Sumber-sumber tersebut dianalisis secara sistematis guna menemukan dasar hukum dan argumentasi normatif atas persoalan yang dikaji.

⁴ Nibert Young, *DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media* United States, 2019.

⁵ Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta : Penerbit Kencana, 2016), hal 93.

⁶ Ishaq, *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, Serta Disertasi*, (Bandung : Alfabeta, 2017), hal 70.

Selanjutnya, teknik analisis data yang digunakan adalah analisis kualitatif, yakni data yang telah dikumpulkan tidak diolah dalam bentuk angka, melainkan dideskripsikan dan dianalisis secara sistematis dan logis untuk menjawab rumusan masalah dan membangun argumen hukum yang rasional.

HASIL DAN PEMBAHASAN

A. Kriteria dan Proses Terjadinya Tindak Pidana Menyerang Kehormatan

Secara umum, kriteria merupakan tolok ukur atau pedoman dalam membuat penilaian atau keputusan hukum, sedangkan proses adalah serangkaian tahapan sistematis untuk mencapai hasil tertentu.⁷ Dalam hal ini, kriteria tindak pidana menyerang kehormatan adalah syarat yang ditentukan oleh hukum untuk menilai apakah suatu perbuatan dapat dikategorikan sebagai perbuatan yang menyerang kehormatan atau nama baik seseorang. Adapun prosesnya mencakup seluruh rangkaian penegakan hukum pidana, mulai dari terjadinya peristiwa pidana hingga pelaku dijatuhi sanksi. Tindak pidana penyerangan terhadap kehormatan diatur dalam Bab XVI KUHP tentang Penghinaan, yang mencakup berbagai bentuk penghinaan, seperti pencemaran lisan atau tulisan (Pasal 310), fitnah (Pasal 311), penghinaan ringan (Pasal 315), pengaduan fitnah (Pasal 317), persangkaan palsu (Pasal 318), serta pencemaran terhadap orang mati (Pasal 320 dan 321). Selain itu, ketentuan serupa juga dimuat dalam Pasal 27A UU RI No. 1 Tahun 2024, yang mengatur bahwa setiap orang yang dengan sengaja menyerang kehormatan atau nama baik orang lain melalui sistem elektronik dapat dipidana.

Contoh nyata dari tindak pidana menyerang kehormatan terjadi pada kasus penyebaran video deepfake yang menampilkan sosok mirip publik figur Nagita Slavina pada Januari 2022. Video tersebut berisi konten vulgar yang secara visual menyerupai korban, meskipun tidak nyata. Konten ini menyebar luas di internet dan menimbulkan persepsi publik yang keliru, sehingga mencemarkan nama baik korban dan merendahkan martabatnya. Tindakan ini memenuhi unsur pelanggaran hukum karena pelaku secara sadar menciptakan dan menyebarkan konten menyesatkan yang merugikan secara reputasi dan emosional. Dalam hal ini, pelaku dapat dikenai pertanggungjawaban pidana berdasarkan Pasal 27A jo Pasal 45 ayat (4) UU RI No. 1 Tahun 2024, dengan ancaman pidana penjara paling lama dua tahun dan/atau denda paling banyak Rp400 juta. Jika konten tersebut mengandung muatan kebencian, maka pelaku juga dapat dikenakan Pasal 28 ayat (2) jo Pasal 45A ayat (2) UU yang sama, dengan ancaman pidana hingga enam tahun penjara dan/atau denda Rp1 miliar. Selain itu, Pasal 310 KUHP juga dapat diterapkan karena unsur pencemaran nama baik terpenuhi.

⁷ <https://kumparan.com/pengertian-dan-istilah/pengertian-proses-fungsi-dan-ciri-cirinya-21Op1gBhugF>

Motivasi pelaku dalam menyebarkan konten semacam ini bisa berasal dari berbagai faktor, antara lain keinginan menarik perhatian publik, motif ekonomi melalui viralitas media sosial, dendam pribadi, atau pengaruh lingkungan sosial yang permisif. Pesatnya perkembangan teknologi digital, khususnya teknologi deepfake, turut memudahkan pelaku dalam menciptakan konten yang menyesatkan dan merugikan pihak lain. Dalam kasus seperti ini, aparat penegak hukum memiliki tanggung jawab untuk menindaklanjuti laporan korban, menyelidiki unsur kesengajaan, serta menegakkan hukum demi memberikan keadilan dan perlindungan atas kehormatan pribadi warga negara sebagaimana dijamin oleh hukum positif di Indonesia.

B. Tanggung Jawab Pidana Menyerang Kehormatan Menurut Pasal 27A UU RI No.1 Tahun 2024

Pertanggungjawaban pidana atau *criminal liability* tidak hanya mencakup aspek hukum, tetapi juga berkaitan dengan nilai moral yang berlaku dalam masyarakat.⁸ Pertanggungjawaban ini berfungsi untuk menentukan apakah seseorang dapat dipidana atas perbuatan yang melanggar hukum. Menurut Roeslan Saleh, hal ini mencakup celaan objektif terhadap perbuatan pidana dan syarat subjektif dari pelaku. Dalam kasus penyebaran video deepfake yang menampilkan sosok mirip Nagita Slavina, secara objektif, perbuatan tersebut merendahkan martabat korban dan menimbulkan persepsi keliru di masyarakat. Jika pelaku menyebarkan video secara sadar, maka unsur subjektif terpenuhi, dan pelaku dapat dimintai pertanggungjawaban pidana.⁹

Teknologi deepfake yang memanfaatkan kecerdasan buatan telah menimbulkan dilema hukum karena memungkinkan manipulasi visual dan audio secara realistis. Meskipun awalnya digunakan untuk hiburan, teknologi ini kini sering disalahgunakan untuk menyebarkan konten yang merugikan, seperti dalam kasus Nagita Slavina. Video tersebut menyebar luas di media sosial, menciptakan kesan seolah korban benar-benar terlibat dalam tindakan tidak senonoh, yang pada akhirnya merusak reputasi dan kondisi psikologis korban. Penyebaran video ini juga dapat berdampak pada kehidupan sosial dan karier korban.

Secara hukum, tindakan tersebut dapat dijerat melalui Pasal 27A UU RI No.1 Tahun 2024, yang menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan informasi elektronik yang menyerang kehormatan atau nama baik orang lain dapat dikenakan sanksi pidana. Unsur-unsur seperti “dengan sengaja”, “tanpa hak”, serta penggunaan informasi dan dokumen elektronik melalui sistem

⁸ Hanafi, Mahrus, *Sisitem Pertanggung Jawaban Pidana*, Cetakan pertama, Jakarta, Rajawali Pers, 2015, hal 16

⁹ Roeslan saleh, *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana*, Cetakan Pertama, Jakarta, Ghalia Indonesia, hal 33

elektronik semuanya terpenuhi dalam kasus ini. Selain itu, pelaku juga dapat dijerat dengan Pasal 310 KUHP tentang pencemaran nama baik sebagai ketentuan umum.

Penegakan hukum terhadap kasus ini harus memperhatikan asas keadilan dan due process of law, serta memperkuat peran negara dalam melindungi kehormatan individu dari serangan digital. Proses hukum yang transparan, berbasis bukti digital yang sah, dan didukung oleh forensik digital sangat diperlukan. Selain menindak pelaku, penegakan hukum juga harus bersifat preventif dan edukatif, agar masyarakat tidak menyalahgunakan teknologi untuk merugikan orang lain. Kolaborasi dengan platform digital juga penting untuk memantau dan menghentikan penyebaran konten yang melanggar hukum. Dengan demikian, penyebaran video deepfake yang menyerang kehormatan individu merupakan tindak pidana yang dapat dipertanggungjawabkan secara hukum berdasarkan Pasal 27A UU RI No.1 Tahun 2024, serta menjadi bukti pentingnya negara hadir untuk melindungi hak atas nama baik sebagai bagian dari hak asasi manusia

KESIMPULAN

Berdasarkan uraian dari hasil penelitian di atas, penulis dapat menyimpulkan sebagai berikut:

1. Berdasarkan kriteria dan proses tindak pidana menyerang kehormatan atau nama baik merupakan salah satu bentuk pelanggaran hukum yang serius dalam sistem hukum pidana Indonesia. Pasal 27A UU RI No.1 Tahun 2024 secara tegas mengatur mengenai perbuatan menyerang kehormatan atau nama baik melalui sarana elektronik, dengan sanksi pidana yang cukup berat. Dalam konteks penyebaran video deepfake yang merugikan Nagita Slavina, perbuatan pelaku telah memenuhi unsur tindak pidana pencemaran nama baik karena dilakukan secara sengaja, menggunakan teknologi, dan disebarkan melalui sistem elektronik kepada khalayak umum. Perbuatan tersebut tidak hanya merendahkan martabat korban, tetapi juga menimbulkan kerugian emosional dan sosial yang signifikan. Oleh karena itu, pelaku dapat dimintai pertanggungjawaban pidana sebagaimana diatur dalam Pasal 27A jo Pasal 45 ayat (4) UU RI No.1 Tahun 2024 dan Pasal 310 KUHP, bahkan Pasal 28 ayat (2) UU ITE jika ditemukan muatan kebencian. Penegakan hukum terhadap kasus seperti ini harus dilaksanakan secara tegas dan profesional, sebagai bentuk perlindungan terhadap kehormatan pribadi serta sebagai upaya untuk mengatasi penyalahgunaan teknologi digital, khususnya teknologi manipulatif seperti deepfake. Dengan demikian, hukum pidana berfungsi tidak hanya sebagai alat represif, tetapi juga sebagai instrumen preventif dan edukatif dalam menjaga nilai-nilai sosial dan martabat kemanusiaan di era digital.
2. Berkenaan dengan tanggung jawab pidana Pelaku penyebaran video menggunakan deepfake yang menyerang kehormatan tindakan tersebut diatur secara tegas dalam

Pasal 27A UU RI No.1 Tahun 2024. Perbuatan pelaku memenuhi unsur pidana, yaitu dilakukan dengan sengaja, tanpa hak, dan menyebarkan informasi elektronik bermuatan pencemaran nama baik melalui sistem elektronik. Selain itu, berdasarkan teori pertanggungjawaban pidana menurut Roeslan Saleh, pelaku dapat dimintai pertanggungjawaban secara hukum karena telah melakukan perbuatan yang secara objektif layak dicela dan secara subjektif dilakukan dengan kesadaran atas akibat yang ditimbulkan. Dampak dari perbuatan ini tidak hanya mencoreng reputasi korban, tetapi juga dapat menimbulkan penderitaan psikis dan kerugian sosial yang serius. Oleh karena itu, penegakan hukum dalam kasus ini harus dilakukan secara profesional, adil, dan menyeluruh, tidak hanya sebagai upaya represif terhadap pelaku, tetapi juga sebagai bentuk perlindungan terhadap hak asasi manusia, khususnya hak atas kehormatan dan nama baik. Negara perlu hadir secara aktif dalam mengawasi dan menanggapi penyalahgunaan teknologi digital agar tidak menjadi alat perusakan karakter individu di ruang publik.

DAFTAR PUSTAKA

- Hanafi, Mahrus, 2016. **Sisitem Pertanggung Jawaban Pidana**, Cetakan pertama, Jakarta, Rajawali Pers.
- Roeslan saleh, **Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana**, Cetakan Pertama, Jakarta, Ghalia Indonesia.
- <https://kumparan.com/pengertian-dan-istilah/pengertian-proses-fungsi-dan-ciri-cirinya-21Op1gBhugF>
- Nobert Young, 2019. **DeepFake Technology: Complete Guide to Deepfakes, Politics and Social**. MediaUnited States.
- Ronny Winarno, Bambang Sudjito, Yudhia Ismail, 2020. **Pengantar Ilmu Hukum**, Malang: Intelegensia Media.
- Santosa, P. I. 2017. **Analisis Data dengan Machine Learning**. Yogyakarta: Andi Offset.
- Peter Mahmud Marzuki, 2016. **Penelitian Hukum**, Jakarta : Penerbit Kencana.
- Ishaq, 2017. **Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, Serta Disertasi**, Bandung : Alfabeta.

Kitab Undang-Undang Hukum Pidana (KUHP).

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

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Bayu Prasetyo, Dkk. 2023 **Recontruction Of Personal Data Protection Law Againts Data Leakage In TheDigitaization Era After The Covid-19 Pandemic**, Lembuswana Law Review: Public Law, Civil Law, Business Law, Vol. 1 No. 1.

Databoks, **Indonesia Penyumbang Kunjungan Aplikasi AI Terbanyakke-3 diDunia**, dalam <https://databoks.katadata.co.id/teknologitelekomunikasi/statistik/a49ed3eb121983b/indonesia-penyumbang-kunjungan-ai-terbanyak-ke-3-di-dunia>, Diakses pada 31 Januari 2024, 13: 23 WIB.