Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 3, 2026
DOI: https://doi.org/10.61104/alz.v4i3.5420

Deepfake Pornografi dan Transformasi Kejahatan Siber di Era AI Generatif

Angelica Suciara[1], Darrel Michelin[2], Giovano Allan Lowa[3], Grace Amaze Huberta[4], Kimberly Fewsan[5], M. Almer Fathoni[6], Meiraate Leos Lediana Tombeg[7], Michelle Regine Maukar[8], Muhamad Bintang Guntoro[9]
Universitas Pelita Harapan, Indonesia[1-9]
Email Korespondensi: wahyuramdhani2204@gmail.com, ribhan@feb.unila.ac.id

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Maret 2026, Article published: 01 Mei 2026

ABSTRACT
The development of generative Artificial Intelligence (AI) has brought significant changes to the digital landscape. The rapid advancement of AI technology has also influenced the patterns of cybercrime. AI enables individuals to create content such as images or videos that appear realistic without requiring advanced technical skills. As a result, cybercrime, which previously required specialized expertise, has become easier to commit with mere access to technology. One form of crime that has emerged as a consequence of this advancement is deepfake pornography, which involves the creation of pornographic content using a person's face or identity without their consent. This study aims to explain how cybercrime has transformed in the era of generative AI, to examine the position of deepfake pornography within this transformation, and to analyze its implications for the legal system in Indonesia. The method used in this research is normative juridical research with a conceptual approach, conducted through library research. The findings indicate that generative AI has shifted the structure of cybercrime from being skill-based to access-based, thereby increasing the potential number of offenders and expanding the scale of such crimes. In addition, existing legal frameworks still face challenges in regulating and addressing technology-based crimes. Therefore, more adaptive legal reforms are needed to keep pace with the rapid development of technology.
Keywords: *Generative AI, deepfake pornography, cybercrime, crime transformation.*

ABSTRAK
Perkembangan Artificial Intelligence (AI) generatif telah membawa perubahan besar dalam dunia digital. Dengan adanya kemajuan teknologi AI yang signifikan membawa berbagai dampak dalam pola kejahatan siber. AI memungkinkan siapa saja untuk membuat konten seperti gambar atau video yang terlihat nyata, tanpa memerlukan keahlian teknis yang tinggi. Akibatnya, kejahatan siber yang sebelumnya membutuhkan keterampilan khusus kini menjadi lebih mudah dilakukan hanya dengan akses terhadap teknologi. Salah satu bentuk kejahatan yang muncul sebagai dampak dari kemajuan AI ini adalah deepfake pornografi, yaitu pembuatan konten pornografi dengan menggunakan wajah atau identitas seseorang tanpa izin. Penelitian ini bertujuan untuk menjelaskan bagaimana kejahatan siber berubah di era AI generatif, bagaimana fenomena deepfake pornografi dalam perubahan tersebut, serta bagaimana dampaknya terhadap sistem hukum di Indonesia. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan konseptual melalui studi

kepustakaan. Hasil penelitian menunjukkan bahwa AI generatif telah mengubah struktur kejahatan siber dari yang berbasis keterampilan menjadi berbasis akses, sehingga jumlah pelaku berpotensi meningkat dan kejahatan menjadi lebih luas penyebarannya. Selain itu, hukum yang ada saat ini masih menghadapi kesulitan dalam mengatur dan menanggulangi kejahatan berbasis teknologi ini. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif agar mampu mengikuti perkembangan teknologi yang semakin cepat.
Kata kunci: *AI generatif, deepfake pornografi, kejahatan siber, transformasi kejahatan.*

PENDAHULUAN

Perkembangan teknologi digital mengalami perkembangan yang sangat pesat, terutama dengan hadirnya Artificial Intelligence (AI) generatif. Teknologi ini memiliki kemampuan untuk menciptakan konten baru berupa teks, gambar, audio, hingga video yang menyerupai realitas. Kehadiran AI generatif tidak hanya meningkatkan efisiensi produksi informasi, tetapi juga mengaburkan batas antara realitas dan manipulasi digital. Kondisi ini menjadikan AI generatif sebagai bentuk disrupsi teknologi yang secara fundamental mengubah cara manusia berinteraksi dengan informasi dan teknologi.

Salah satu karakter utama dari perkembangan AI generatif adalah semakin mudahnya teknologi ini diakses dan digunakan oleh masyarakat luas. Teknologi yang sebelumnya membutuhkan keahlian teknis tinggi kini dapat dimanfaatkan oleh hampir semua orang, bahkan tanpa latar belakang teknis atau keahlian yang mendalam dalam bidang teknologi.

Melalui berbagai platform yang tersedia, individu dapat menghasilkan konten kompleks hanya dengan memberikan perintah sederhana (prompt). Kemudahan yang diberikan sebagai dampak perkembangan era digital ini di satu sisi mendorong inovasi dan memperluas partisipasi masyarakat dalam pemanfaatan teknologi, namun di sisi lain juga membuka peluang besar bagi penyalahgunaan teknologi, khususnya dalam konteks kejahatan siber.

Perkembangan tersebut berdampak langsung pada transformasi kejahatan siber. Kejahatan yang sebelumnya berbasis keterampilan (skill-based crime) kini beralih menjadi kejahatan berbasis akses (access-based crime). Pelaku tidak lagi memerlukan kemampuan teknis yang kompleks, melainkan cukup memanfaatkan teknologi yang tersedia secara luas. Transformasi ini menyebabkan meningkatnya jumlah pelaku potensial serta memperluas skala dan dampak kejahatan di ruang digital.

Salah satu bentuk kejahatan yang paling merepresentasikan perubahan tersebut adalah deepfake pornografi. Teknologi deepfake memungkinkan manipulasi wajah dan identitas seseorang ke dalam konten audiovisual secara realistis menggunakan AI, hal ini dilakukan dengan cara menggunakan AI untuk mengambil, mengumpulkan dan menggunakan foto dan video orang lain dan mengubahnya menjadi konten yang telah dimanipulasi. Dalam praktiknya seringkali hal dilakukan dengan tujuan membuat konten pornografi yang melibatkan identitas seseorang tanpa persetujuan. Hal ini tidak hanya melanggar privasi, tetapi juga berdampak pada kehormatan, reputasi, serta kondisi psikologis

korban. Perkembangan teknologi ini juga menimbulkan tantangan serius dalam aspek pembuktian dan penegakan hukum, karena sifatnya yang sulit dideteksi dan dilacak.

Dalam konteks hukum Indonesia, pengaturan terkait kejahatan siber dan perlindungan individu sebenarnya telah diatur dalam beberapa peraturan perundang-undangan yang masih berlaku. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur berbagai perbuatan yang dilarang dalam ruang digital, termasuk distribusi konten yang melanggar kesusilaan serta penghinaan melalui media elektronik. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan perlindungan terhadap data pribadi, termasuk data biometrik seperti wajah yang menjadi objek utama dalam teknologi deepfake.

Namun demikian, perkembangan teknologi deepfake menunjukkan bahwa hukum positif di Indonesia masih belum sepenuhnya mampu mengakomodasi bentuk-bentuk kejahatan baru yang muncul akibat AI generatif. Belum adanya pengaturan yang secara spesifik mengatur deepfake menyebabkan munculnya celah hukum, baik dalam perlindungan korban maupun dalam proses penegakan hukum. Kondisi ini menunjukkan adanya kesenjangan antara perkembangan teknologi dan kesiapan sistem hukum dalam meresponsnya.

Dengan demikian, dapat dipahami bahwa AI generatif tidak hanya mengubah alat yang digunakan dalam kejahatan siber, tetapi juga mengubah struktur dan karakter kejahatan itu sendiri. Kejahatan tidak lagi bergantung pada kemampuan teknis, melainkan pada kemudahan akses terhadap teknologi. Deepfake pornografi dalam hal ini menjadi representasi nyata dari transformasi tersebut, sekaligus menunjukkan pentingnya pembaruan hukum yang lebih adaptif.

Berdasarkan uraian tersebut, penelitian ini berfokus pada analisis transformasi kejahatan siber di era AI generatif dengan menempatkan deepfake pornografi sebagai fenomena utama. Permasalahan yang dikaji meliputi bagaimana transformasi kejahatan siber terjadi, bagaimana posisi deepfake pornografi dalam transformasi tersebut, serta bagaimana implikasinya terhadap sistem hukum di Indonesia. Kajian ini diharapkan dapat memberikan kontribusi dalam pengembangan hukum yang lebih responsif terhadap dinamika kejahatan siber di era teknologi yang terus berkembang.

METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian yang berfokus pada analisis norma hukum yang berlaku serta konsep-konsep hukum yang relevan dengan permasalahan yang dikaji. Pendekatan yang digunakan adalah pendekatan konseptual (conceptual approach), yang bertujuan untuk memahami dan menganalisis konsep-konsep utama seperti kejahatan siber, AI generatif, serta deepfake dalam kerangka teoritis Bahan hukum yang digunakan dalam penelitian ini terdiri dari bahan hukum primer dan bahan hukum sekunder.

Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan kejahatan siber, teknologi informasi, serta perlindungan terhadap individu, sedangkan bahan hukum sekunder meliputi literatur ilmiah, jurnal akademik, serta hasil penelitian yang relevan dengan topik AI generatif dan transformasi kejahatan siber. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), dengan menelaah berbagai sumber yang memiliki relevansi dan kredibilitas akademik. Melalui metode ini, diharapkan dapat diperoleh pemahaman yang komprehensif mengenai perubahan struktur kejahatan serta implikasinya terhadap sistem hukum di era AI generatif.

HASIL DAN PEMBAHASAN

Bagaimana transformasi kejahatan siber di era Artificial Intelligence (AI) generatif?

Perkembangan teknologi Artificial Intelligence (AI) dalam beberapa tahun terakhir telah menjadi salah satu faktor utama yang mendorong perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam bidang kejahatan siber. AI tidak hanya menghadirkan inovasi dalam efisiensi dan produktivitas, tetapi juga membuka peluang baru bagi munculnya bentuk-bentuk kejahatan yang lebih kompleks, terstruktur, dan sulit dideteksi. Dalam konteks ini, kejahatan siber mengalami transformasi mendasar yang tidak hanya berkaitan dengan alat yang digunakan, tetapi juga menyangkut perubahan dalam struktur, pola, dan karakteristik kejahatan itu sendiri.10 Transformasi tersebut salah satunya ditandai dengan meningkatnya kemampuan teknologi dalam melakukan otomatisasi dan analisis data dalam skala besar. AI memungkinkan pengolahan informasi secara cepat dan akurat, termasuk dalam mengidentifikasi pola, memprediksi perilaku, dan menyesuaikan strategi secara real-time. Dalam konteks kejahatan siber, kemampuan ini dimanfaatkan oleh pelaku untuk meningkatkan efektivitas serangan, baik dalam bentuk pencurian data, penipuan digital, maupun manipulasi informasi.

Salah satu perubahan paling signifikan dalam kejahatan siber adalah pergeseran dari skill-based crime menuju access-based crime. Pada masa sebelumnya, kejahatan siber hanya dapat dilakukan oleh individu dengan keahlian teknis tinggi, seperti penguasaan bahasa pemrograman, sistem jaringan, dan teknik enkripsi. Namun, dengan berkembangnya AI, berbagai alat dan platform berbasis teknologi kini tersedia secara luas dan mudah diakses oleh masyarakat umum.12 Hal ini menyebabkan penurunan hambatan teknis dalam melakukan kejahatan, sehingga memperluas basis pelaku potensial. Muhamad Nur Ismail, Pengaruh Teknologi AI terhadap Evolusi Modus Kejahatan Siber di Indonesia Tahun 2024–2025 dan Implikasinya terhadap Penegakan Hukum, hlm. Cindy Tania & Janwan Gidalty, Strategi Penuntutan Kejahatan Siber dengan Artificial Intelligence di Era Digital, hlm. 1387–1388.

Muhamad Nur Ismail, Pengaruh Teknologi AI terhadap Evolusi Modus Kejahatan Siber di Indonesia Tahun 2024–2025 dan Implikasinya terhadap Penegakan Hukum Perubahan ini berdampak langsung terhadap meningkatnya

kuantitas kejahatan siber. Ketika akses terhadap teknologi menjadi semakin mudah, maka kemungkinan terjadinya kejahatan juga meningkat secara eksponensial. AI memungkinkan individu dengan kemampuan minimal untuk melakukan tindakan kriminal yang sebelumnya hanya dapat dilakukan oleh kelompok tertentu. Dengan demikian, transformasi ini tidak hanya meningkatkan jumlah pelaku, tetapi juga memperluas skala dan dampak kejahatan di ruang digital.13

Selain itu, AI juga memungkinkan terjadinya otomatisasi dalam pelaksanaan kejahatan. Serangan siber tidak lagi bergantung pada intervensi manusia secara langsung, melainkan dapat dijalankan secara sistematis melalui algoritma yang dirancang untuk melakukan tindakan tertentu.14 Misalnya, sistem berbasis AI dapat digunakan untuk melakukan serangan phishing secara massal dengan menyesuaikan pesan terhadap karakteristik target, sehingga meningkatkan tingkat keberhasilan serangan. Hal ini menunjukkan bahwa AI telah mengubah kejahatan siber menjadi lebih efisien dan terorganisir.

Lebih jauh lagi, perkembangan AI telah melahirkan berbagai modus kejahatan baru yang semakin kompleks. Kejahatan siber kini mencakup berbagai bentuk seperti deepfake-based fraud, phishing adaptif berbasis machine learning, serta ransomware yang dihasilkan secara otomatis oleh sistem AI. Modus-modus ini tidak hanya menunjukkan peningkatan dalam kompleksitas teknis, tetapi juga memperlihatkan kemampuan AI dalam menciptakan strategi kejahatan yang lebih canggih dan sulit diprediksi.

Transformasi ini juga berdampak pada peningkatan kualitas kejahatan siber. Jika sebelumnya kejahatan dilakukan secara sederhana dan terbatas, kini kejahatan dapat dilakukan secara terstruktur dan terkoordinasi dengan memanfaatkan teknologi AI. Algoritma dapat digunakan untuk mengidentifikasi celah keamanan, memetakan target, serta menentukan strategi serangan yang paling efektif. Bahkan, dalam beberapa kasus, AI mampu melakukan pembelajaran dari serangan sebelumnya untuk meningkatkan efektivitas serangan berikutnya.15 Di sisi lain, perkembangan ini juga menimbulkan tantangan serius dalam aspek pembuktian hukum. Kejahatan berbasis AI sering kali menghasilkan bukti Muhamad Nur Ismail, Pengaruh Teknologi AI terhadap Evolusi Modus Kejahatan Siber di Indonesia Tahun 2024–2025 dan Implikasinya terhadap Penegakan Hukum, hlm Siti Nurkholisah et al., Tantangan Kriminalisasi Deepfake dalam Hukum Pidana Indonesia, hlm. 2421–2422. Siti Nurkholisah et al., Tantangan Kriminalisasi Deepfake dalam Hukum Pidana Indonesia, digital yang kompleks dan sulit diverifikasi. Konten yang dihasilkan oleh AI dapat menyerupai realitas secara sangat akurat, sehingga menyulitkan aparat penegak hukum dalam membedakan antara konten asli dan manipulasi. Hal ini berdampak pada meningkatnya kesulitan dalam proses pembuktian, yang merupakan salah satu elemen penting dalam sistem peradilan pidana.16

Selain itu, keterbatasan dalam teknologi forensik digital juga menjadi kendala dalam penanganan kejahatan siber berbasis AI. Aparat penegak hukum seringkali belum memiliki alat dan kemampuan yang memadai untuk menganalisis bukti digital yang kompleks. Keterbatasan ini diperparah dengan kurangnya

sumber daya manusia yang memiliki keahlian khusus di bidang teknologi informasi dan kecerdasan buatan. Akibatnya, efektivitas penegakan hukum terhadap kejahatan siber berbasis AI masih belum optimal.

Transformasi kejahatan siber juga menimbulkan tantangan dalam aspek yurisdiksi hukum. Kejahatan siber bersifat lintas batas negara (borderless crime), sehingga pelaku dapat beroperasi dari berbagai wilayah tanpa terikat oleh batas geografis. Hal ini menyulitkan proses penegakan hukum, terutama dalam hal penentuan yurisdiksi dan kerja sama antar negara. Tanpa adanya koordinasi internasional yang efektif, penanganan kejahatan siber akan menghadapi hambatan yang signifikan. Lebih dari itu, perkembangan AI juga menunjukkan bahwa kejahatan siber tidak lagi bersifat reaktif, tetapi telah berkembang menjadi proaktif dan prediktif. Pelaku dapat memanfaatkan AI untuk menganalisis data target sebelum melakukan serangan, sehingga meningkatkan peluang keberhasilan. Hal ini menunjukkan bahwa kejahatan siber telah mengalami evolusi dari sekadar tindakan oportunistik menjadi strategi yang dirancang secara sistematis.

Dalam perspektif hukum, kondisi ini menunjukkan adanya kesenjangan antara perkembangan teknologi dengan kesiapan sistem hukum dalam meresponsnya. Regulasi yang ada saat ini pada umumnya masih bersifat reaktif dan belum sepenuhnya mampu mengakomodasi karakteristik kejahatan berbasis AI yang kompleks dan dinamis. Kurangnya definisi hukum yang jelas, keterbatasan dalam pembuktian, serta belum optimalnya koordinasi antar lembaga menjadi faktor yang menghambat efektivitas penegakan hukum.

Dengan demikian, dapat disimpulkan bahwa perkembangan AI telah mengubah secara fundamental struktur dan karakter kejahatan siber. Transformasi ini mencakup perubahan dalam pelaku, modus operandi, skala, serta dampak kejahatan. Kejahatan siber tidak lagi bergantung pada kemampuan teknis semata, melainkan pada kemudahan akses terhadap teknologi yang semakin luas. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif dan responsif agar mampu menghadapi dinamika kejahatan siber di era AI generatif.

Bagaimana posisi dan karakteristik deepfake pornografi dalam transformasi kejahatan siber tersebut?

Dalam konteks transformasi kejahatan siber di era Artificial Intelligence (AI), deepfake pornografi menempati posisi yang sangat strategis sebagai salah satu bentuk kejahatan digital yang paling berkembang dan kompleks. Deepfake pornografi bukan hanya sekadar variasi dari kejahatan siber, melainkan representasi nyata dari bagaimana teknologi AI telah mengubah paradigma kejahatan, baik dari segi metode, dampak, maupun tingkat kesulitannya dalam penanganan hukum.17

Secara konseptual, deepfake pornografi merupakan bentuk kejahatan yang memanfaatkan teknologi AI untuk memanipulasi gambar atau video seseorang tanpa persetujuan, sehingga menghasilkan konten pornografi yang tampak realistis. Teknologi ini bekerja dengan teknik deep learning yang mampu memindai dan merekonstruksi wajah atau tubuh seseorang ke dalam konten lain, sehingga

menghasilkan visual yang sulit dibedakan dari kenyataan.18 Dengan demikian, deepfake pornografi memiliki karakteristik utama berupa manipulasi identitas digital yang sangat akurat dan menyesatkan. Posisi deepfake pornografi dalam transformasi kejahatan siber dapat dipahami sebagai bentuk evolusi dari kejahatan berbasis konten (content-based crime). Jika sebelumnya kejahatan pornografi digital dilakukan melalui distribusi konten nyata, maka dalam deepfake pornografi, konten tersebut sepenuhnya dapat direkayasa. Hal ini menunjukkan bahwa kejahatan tidak lagi bergantung pada realitas, tetapi dapat diciptakan secara artifisial melalui teknologi.

Karakteristik lain yang menonjol dari deepfake pornografi adalah sifatnya yang non-konsensual, yaitu penggunaan identitas seseorang tanpa izin. Dalam banyak kasus, korban tidak pernah terlibat dalam pembuatan konten tersebut, namun wajah atau identitasnya dimasukkan ke dalam konten pornografi. Hal ini menyebabkan dampak yang sangat serius terhadap korban, terutama dalam aspek kehormatan, privasi, dan reputasi. Bahkan, dalam perspektif hukum, tindakan ini dapat dikategorikan sebagai bentuk pencemaran nama baik karena memenuhi unsur merusak kehormatan seseorang melalui media digital.19

Deepfake pornografi juga memiliki karakteristik sebagai kejahatan berbasis teknologi tinggi (high-tech crime) yang sulit dideteksi. Konten yang dihasilkan memiliki tingkat realisme yang sangat tinggi, sehingga sulit dibedakan antara konten asli dan manipulasi. Hal ini menimbulkan tantangan besar dalam proses pembuktian hukum, karena aparat penegak hukum harus mampu membuktikan bahwa konten tersebut merupakan hasil rekayasa teknologi, bukan kejadian nyata.20

Deepfake pornografi juga memiliki karakteristik sebagai kejahatan yang sangat cepat dan masif. Kemudahan distribusi melalui media sosial dan platform digital menyebabkan konten dapat menyebar dalam waktu singkat dan menjangkau audiens yang luas. Bahkan, berdasarkan data yang ditunjukkan dalam penelitian, mayoritas konten deepfake yang beredar di internet adalah konten pornografi, dengan persentase mencapai lebih dari 90%. Hal ini menunjukkan bahwa deepfake pornografi merupakan bentuk dominan dalam penggunaan teknologi deepfake secara negatif.21 Deepfake pornografi juga memiliki karakteristik sebagai kejahatan yang bersifat gendered crime, di mana sebagian besar korbannya adalah perempuan. Hal ini menunjukkan adanya dimensi ketidaksetaraan gender dalam kejahatan siber berbasis AI. Deepfake pornografi tidak hanya menjadi masalah teknologi, tetapi juga berkaitan dengan isu sosial, seperti kekerasan berbasis gender online (KBGO) yang semakin meningkat dalam beberapa tahun terakhir.

Dari perspektif hukum, posisi deepfake pornografi juga menunjukkan adanya kekosongan hukum (legal vacuum). Regulasi yang ada, seperti KUHP, UU ITE, dan UU TPKS, pada dasarnya belum secara spesifik mengatur mengenai deepfake. Akibatnya, penanganan kasus deepfake pornografi sering kali menggunakan pasal-pasal umum yang tidak sepenuhnya mampu mengakomodasi

karakteristik kejahatan ini. Hal ini berdampak pada lemahnya perlindungan hukum terhadap korban serta kesulitan dalam proses penegakan hukum.

Karakteristik deepfake pornografi juga berkaitan dengan sifat kejahatan siber yang lintas batas negara (borderless crime). Konten dapat dibuat di satu negara dan disebarkan ke berbagai negara lain tanpa batasan geografis. Hal ini menimbulkan tantangan dalam hal yurisdiksi hukum serta kerja sama internasional dalam penanganan kejahatan.22 Dalam perspektif yang lebih luas, deepfake pornografi dapat dipandang sebagai bentuk kejahatan yang menggabungkan berbagai elemen kejahatan siber, yaitu manipulasi data, pelanggaran privasi, pencemaran nama baik, serta kekerasan seksual berbasis digital. Kombinasi ini menjadikan deepfake pornografi sebagai salah satu bentuk kejahatan yang paling kompleks dalam era digital.

Dengan demikian, posisi deepfake pornografi dalam transformasi kejahatan siber dapat dikatakan sebagai bentuk kejahatan yang berada di persimpangan antara teknologi, hukum, dan sosial. Karakteristiknya yang unikmulai dari manipulasi identitas, non-konsensual, realisme tinggi, hingga penyebaran masifmenjadikannya sebagai tantangan serius bagi sistem hukum modern. Oleh karena itu, diperlukan pendekatan yang komprehensif, baik dari sisi regulasi, teknologi, maupun kesadaran masyarakat, untuk dapat mengatasi fenomena ini secara efektif.

Bagaimana implikasi keberadaan deepfake pornografi terhadap sistem hukum di Indonesia?

Keberadaan deepfake pornografi memberikan implikasi signifikan terhadap sistem hukum di Indonesia, terutama dalam aspek regulasi, pembuktian, dan perlindungan hukum. Salah satu implikasi utama adalah adanya kekosongan hukum (legal vacuum) karena belum terdapat aturan yang secara spesifik mengatur deepfake sebagai tindak pidana tersendiri. Regulasi yang ada seperti KUHP, UU ITE, dan UU TPKS masih bersifat umum dan belum mampu mengakomodasi kompleksitas kejahatan berbasis AI.23

Akibatnya, penanganan kasus deepfake pornografi sering menggunakan pasal-pasal umum seperti pencemaran nama baik atau pelanggaran kesusilaan, yang menimbulkan ketidakpastian hukum. Selain itu, deepfake pornografi juga menimbulkan kesulitan pembuktian, karena konten yang dihasilkan sangat realistis sehingga sulit dibedakan antara asli dan manipulasi, sementara kemampuan forensik digital masih terbatas. Implikasi lainnya adalah lemahnya perlindungan terhadap korban, yang sering mengalami kerugian reputasi, psikologis, dan sosial tanpa perlindungan hukum yang memadai.24 Di sisi lain, aparat penegak hukum juga menghadapi keterbatasan dalam hal teknologi dan keahlian, sehingga penegakan hukum belum optimal.

Deepfake pornografi berkaitan dengan pelanggaran hak privasi dan kehormatan, serta memiliki sifat lintas batas negara (borderless crime) yang menyulitkan penegakan hukum.25 Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif, termasuk pengaturan khusus mengenai deepfake serta penguatan kapasitas penegak hukum dan teknologi forensik digital.

Lebih lanjut, implikasi deepfake pornografi juga terlihat dalam aspek kepercayaan publik terhadap sistem hukum dan informasi digital. Kemampuan teknologi deepfake dalam menciptakan konten yang sangat realistis berpotensi menimbulkan disinformasi dan merusak kepercayaan masyarakat terhadap keaslian suatu bukti digital. Hal ini tidak hanya berdampak pada individu sebagai korban, tetapi juga dapat memengaruhi stabilitas sosial dan legitimasi lembaga hukum apabila bukti digital tidak lagi dianggap kredibel.

Selain itu, keberadaan deepfake pornografi menunjukkan urgensi pendekatan hukum yang tidak hanya bersifat represif, tetapi juga preventif dan edukatif. Peningkatan literasi digital masyarakat menjadi penting agar individu mampu mengenali dan menghindari penyalahgunaan teknologi. Di sisi lain, negara juga perlu mendorong kolaborasi antara pemerintah, platform digital, dan masyarakat dalam mengendalikan penyebaran konten deepfake, sehingga penanganan kejahatan ini tidak hanya bergantung pada penegakan hukum semata, tetapi juga pada kesadaran kolektif26.

SIMPULAN

Perkembangan Artificial Intelligence (AI) generatif telah mendorong terjadinya transformasi mendasar dalam kejahatan siber, yang ditandai dengan pergeseran dari kejahatan berbasis keterampilan (skill-based crime) menjadi kejahatan berbasis akses (access-based crime). Kemudahan akses terhadap teknologi memungkinkan individu tanpa keahlian teknis tinggi untuk melakukan kejahatan siber, sehingga meningkatkan jumlah pelaku, memperluas skala kejahatan, serta memperumit pola dan modus operandi yang digunakan. Dalam konteks tersebut, deepfake pornografi menempati posisi sebagai salah satu bentuk kejahatan yang paling merepresentasikan transformasi tersebut. Karakteristiknya yang memanfaatkan manipulasi identitas secara realistis melalui teknologi AI menjadikannya tidak hanya sebagai pelanggaran terhadap privasi dan kehormatan individu, tetapi juga sebagai ancaman serius yang sulit dideteksi dan dibuktikan dalam proses hukum. Hal ini menunjukkan bahwa perkembangan teknologi telah melampaui kesiapan instrumen hukum yang ada. Implikasinya terhadap sistem hukum di Indonesia menunjukkan adanya kesenjangan antara perkembangan teknologi dan regulasi yang berlaku. Meskipun telah terdapat pengaturan melalui UU ITE dan UU Perlindungan Data Pribadi, belum adanya ketentuan spesifik mengenai deepfake menyebabkan lemahnya perlindungan hukum bagi korban serta kendala dalam penegakan hukum. Oleh karena itu, diperlukan pembaruan hukum yang lebih adaptif dan responsif agar mampu mengakomodasi perkembangan kejahatan siber berbasis AI serta memberikan perlindungan yang efektif bagi masyarakat.

DAFTAR RUJUKAN

Badan Siber dan Sandi Negara (BSSN). Laporan Tahunan Keamanan Siber Indonesia 2023. Jakarta: BSSN, 2023.

Basah, Desty Aster Yansen, Andika Wijaya, dan Ivans Januardy. Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana terhadap Penyebaran Deepfake di Media Sosial. Jurnal Innovative: Journal of Social Science Research.

Berlian, Cheny. Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan Artificial Intelligence. Disertasi, Universitas Jambi, 2025.

Daulay, Renjana Mantri Laras Hadi, Rosmalinda, dan Agusmidah. Fenomena Kejahatan Deepfake Pornografi dalam Perspektif Roscoe Pound. Jurnal Pengabdian Masyarakat dan Riset Pendidikan.

Irawati, Nurulhuda, Ismansyah, dan Nani Mulyati. Pertanggungjawaban Pidana Deepfake Porn Berbasis AI: Studi Perbandingan dan Implikasi Global. Jurnal Hukum Lex Generalis.

Ismail, Muhamad Nur. Pengaruh Teknologi AI terhadap Evolusi Modus Kejahatan Siber di Indonesia Tahun 2024–2025 dan Implikasinya terhadap Penegakan Hukum. Jurnal JICN Nusantara.

Kementerian Komunikasi dan Informatika Republik Indonesia. Perkembangan Teknologi Kecerdasan Artifisial di Indonesia. Jakarta: Kominfo, 2023.

Nurkholisah, Siti, et al. Tantangan Kriminalisasi Deepfake dalam Hukum Pidana Indonesia. Jurnal USM Law Review.

Pratama, I Putu Agus Eka. Cyber Security dan Cyber Crime Berbasis Teknologi Terkini. Bandung: Informatika, 2021.

Rahardjo, Budi. "Tantangan Keamanan Siber di Era Artificial Intelligence."
Jurnal Keamanan Informasi Indonesia.

Sari, Dwi Putri. "Implikasi Hukum Penggunaan Deepfake dalam Kejahatan Siber di Indonesia." Jurnal Hukum Digital Indonesia.

Sijabat, Sarah Amanda Uly, dan Diana Lukitasari. Konten Gambar dan Video Pornografi Deepfake sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik. Jurnal Recidive.

Tania, Cindy, dan Janwan Gidalty. Strategi Penuntutan Kejahatan Siber dengan Artificial Intelligence di Era Digital. Jurnal Ilmu Hukum dan Sosial (HAKIM).

