ALADALAH : Jurnal Politik, Sosial, Hukum dan Humaniora
Volume 4 Nomor 2 2026
P-ISSN: 2962-889X; E-ISSN: 2962-8903
DOI: https://doi.org/10.59246/aladalah.v2i4
Tersedia online di: https://ejurnalqarnain.stisnq.ac.id/index.php/ALADALAH

.

Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana

Bintang Muhammad Akbar[1*], Rena Yulia[2], Muhamad Romdoni[3]

[1.2.3] Fakultas Hukum, Univeristas Sultan Ageng Tirtayasa, Indonesia
*Email: bintangma2003@gmail.com[1], rena.yulia@gmail.com[2], muhamadromdoni@untirta.ac.id[3]

Alamat: Jl. Raya Palka Km 3, Sindangsari, Kec. Pabuaran, Kabupaten Serang, Banten 42111, Indonesia
Korespondensi penulis: bintangma2003@gmail.com

Abstract. *The rapid advancement of artificial intelligence, particularly deepfake technology, has generated complex challenges for criminal law enforcement in Indonesia. Deepfake technology enables highly realistic manipulation of audio-visual content, increasing the risk of defamation, fraud, disinformation, identity misuse, and other forms of cybercrime. Although the Indonesian Law on Electronic Information and Transactions (ITE Law) regulates electronic information and data manipulation, its provisions remain general and have not explicitly addressed the specific characteristics, risks, and legal implications of AI-generated synthetic content. This normative gap has led to legal uncertainty, difficulties in criminal qualification, challenges in digital evidence verification, and ambiguity in determining criminal liability, especially in cases involving deepfake-based hoaxes. Through a normative juridical analysis supported by statutory, conceptual, and comparative approaches, this article highlights the limitations of the current ITE Law framework in responding to the evolving nature of deepfake misuse. Comparative insights from the European Union's AI Act and China's Deep Synthesis Provisions demonstrate more adaptive, risk-based, and preventive regulatory models. The findings underline the urgency of reformulating the ITE Law to explicitly regulate deepfake content, strengthen legal certainty, integrate preventive mechanisms such as transparency and platform responsibility, and align criminal law policy with technological developments. Such reformulation is essential to ensure effective law enforcement, protect fundamental rights, and maintain public trust in the digital ecosystem..*

Keywords: *Artificial intelligence; criminal law reform; deepfake; ITE Law; cybercrime.*

Abstrak. Perkembangan pesat kecerdasan buatan, khususnya teknologi deepfake, menghadirkan tantangan serius bagi sistem hukum pidana di Indonesia. Teknologi ini memungkinkan manipulasi konten audio-visual secara sangat realistis sehingga berpotensi menimbulkan pencemaran nama baik, penipuan, penyebaran disinformasi, pencurian identitas, serta berbagai bentuk kejahatan siber lainnya. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur informasi elektronik dan manipulasi data, pengaturannya masih bersifat umum dan belum secara eksplisit mengakomodasi karakteristik serta risiko khusus konten sintetis berbasis kecerdasan buatan. Kondisi tersebut menimbulkan ketidakpastian hukum, kesulitan pembuktian digital, serta persoalan dalam penentuan pertanggungjawaban pidana pelaku penyalahgunaan deepfake. Melalui analisis yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif, artikel ini

* Bintang Muhammad Akbar, bintangma2003@gmail.com

mengidentifikasi kelemahan substantif UU ITE dalam merespons kejahatan berbasis deepfake. Perbandingan dengan pengaturan di Uni Eropa dan China menunjukkan pentingnya pendekatan adaptif, berbasis risiko, serta penekanan pada mekanisme pencegahan dan tanggung jawab platform digital. Temuan ini menegaskan urgensi reformulasi UU ITE guna memberikan kepastian hukum, memperkuat perlindungan masyarakat, serta memastikan hukum pidana nasional mampu beradaptasi dengan perkembangan teknologi kecerdasan buatan.

Kata kunci: *deepfake;* kecerdasan buatan; kejahatan siber; pembaharuan hukum pidana, Undang-Undang ITE.

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (artificial intelligence/AI) telah membawa perubahan signifikan dalam berbagai aspek kehidupan sosial, ekonomi, dan hukum. Salah satu manifestasi AI yang paling menonjol dan problematis adalah teknologi deepfake, yaitu teknik manipulasi konten audio-visual berbasis pembelajaran mesin yang mampu menghasilkan representasi palsu dengan tingkat realisme tinggi (Jaya et al., 2018). Kemampuan tersebut menjadikan deepfake tidak hanya sebagai inovasi teknologi, tetapi juga sebagai potensi instrumen kejahatan siber. Dalam konteks hukum pidana, fenomena ini menimbulkan tantangan baru karena karakter kejahatan yang dihasilkan berbeda dari tindak pidana konvensional. Oleh karena itu, kehadiran deepfake menuntut respons hukum yang adaptif dan berorientasi pada perlindungan masyarakat digital.

Penyalahgunaan deepfake telah digunakan dalam berbagai bentuk kejahatan, seperti pencemaran nama baik, penipuan, pemerasan, penyebaran hoaks, dan pelanggaran hak privasi. Teknologi ini memungkinkan pelaku memanipulasi wajah, suara, dan ekspresi seseorang sehingga menghasilkan konten palsu yang sulit dibedakan dari konten asli (Wahyudi, 2025). Dampaknya tidak hanya bersifat individual, tetapi juga kolektif, karena dapat merusak kepercayaan publik, memengaruhi opini masyarakat, dan mengganggu stabilitas sosial-politik. Karakter ruang siber yang lintas batas turut memperumit proses penegakan hukum terhadap kejahatan ini. Situasi tersebut

memperlihatkan bahwa deepfake bukan sekadar isu teknis, melainkan persoalan hukum pidana yang kompleks dan multidimensional.

Di Indonesia, pengaturan mengenai kejahatan siber masih bertumpu pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Meskipun UU ITE mengatur informasi elektronik, manipulasi data, serta perbuatan melawan hukum di ruang digital, norma yang ada belum secara eksplisit mengatur teknologi deepfake sebagai produk AI (Respati, 2024a). Ketentuan yang bersifat umum ini menimbulkan persoalan kepastian hukum, khususnya dalam menentukan unsur tindak pidana, pembuktian digital, serta pertanggungjawaban pidana pelaku. Akibatnya, aparat penegak hukum kerap mengalami kesulitan dalam mengkualifikasikan perbuatan deepfake ke dalam pasal-pasal yang tersedia. Kondisi ini menunjukkan adanya kesenjangan antara perkembangan teknologi (das sein) dan pengaturan hukum yang berlaku (das sollen).

Sejumlah penelitian sebelumnya telah membahas deepfake dari perspektif perlindungan korban, kriminalisasi, maupun etika penggunaan AI. Namun, sebagian besar kajian tersebut masih berfokus pada aspek deskriptif atau sektoral, seperti deepfake porn atau pelanggaran privasi, tanpa mengaitkannya secara sistematis dengan kebutuhan reformulasi hukum pidana nasional (Noerman & Ibrahim, 2024; Kusnadi & Putri, 2025). Selain itu, kajian komparatif terhadap pengaturan deepfake di negara lain sering kali belum dimanfaatkan secara optimal sebagai dasar pembaruan regulasi di Indonesia. Dengan demikian, masih terdapat kekosongan penelitian yang menempatkan deepfake sebagai dasar urgensi reformulasi UU ITE dalam kerangka pembaharuan hukum pidana secara menyeluruh. Kekosongan inilah yang menjadi celah akademik yang perlu diisi.

Berdasarkan permasalahan tersebut, pembaharuan hukum pidana melalui reformulasi UU ITE menjadi kebutuhan yang tidak dapat dihindari. Reformulasi ini tidak hanya ditujukan untuk menutup kekosongan norma, tetapi juga untuk

membangun sistem hukum yang adaptif, preventif, dan responsif terhadap perkembangan teknologi AI. Pengalaman negara lain, seperti Uni Eropa dan China, menunjukkan bahwa pengaturan berbasis risiko, transparansi, dan tanggung jawab platform digital dapat menjadi instrumen efektif dalam mengendalikan penyalahgunaan deepfake (Respati, 2024b). Oleh karena itu, pendahuluan ini menegaskan urgensi pembahasan reformulasi UU ITE sebagai bagian dari strategi pembaharuan hukum pidana Indonesia di era kecerdasan buatan.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian hukum yang menitikberatkan pada analisis norma hukum tertulis dan doktrin hukum yang relevan. Pendekatan ini dipilih karena fokus penelitian terletak pada evaluasi dan reformulasi norma dalam Undang-Undang Informasi dan Transaksi Elektronik terhadap penyalahgunaan teknologi deepfake. Penelitian yuridis normatif memungkinkan peneliti untuk mengkaji kesesuaian antara norma hukum yang berlaku dengan perkembangan teknologi kecerdasan buatan. Selain itu, metode ini relevan untuk menilai kecukupan regulasi dalam memberikan kepastian hukum dan perlindungan masyarakat. Dengan demikian, penelitian ini tidak berorientasi pada pengumpulan data empiris lapangan, melainkan pada analisis hukum secara konseptual dan sistematis.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah ketentuan UU ITE, Undang-Undang Perlindungan Data Pribadi, serta peraturan lain yang berkaitan dengan kejahatan siber dan teknologi AI. Pendekatan konseptual digunakan untuk memahami konsep deepfake, kecerdasan buatan, pertanggungjawaban pidana, dan pembaharuan hukum pidana yang berkembang dalam literatur hukum. Melalui pendekatan ini, penelitian mampu mengidentifikasi kelemahan normatif serta implikasi yuridis

dari ketiadaan pengaturan eksplisit mengenai deepfake. Pendekatan ini juga membantu membangun kerangka analisis yang konsisten dengan teori hukum pidana modern.

Selain itu, penelitian ini menggunakan pendekatan komparatif (comparative approach) untuk memperkaya analisis normatif. Pendekatan ini dilakukan dengan membandingkan pengaturan deepfake dan AI di Indonesia dengan regulasi di Uni Eropa melalui EU Artificial Intelligence Act dan di China melalui Provisions on the Administration of Deep Synthesis of Internet-based Information Services. Perbandingan ini bertujuan untuk mengidentifikasi prinsip-prinsip pengaturan yang adaptif dan relevan untuk konteks Indonesia. Hasil perbandingan tersebut digunakan sebagai bahan pertimbangan dalam merumuskan arah reformulasi UU ITE. Dengan demikian, metode penelitian ini mendukung penyusunan rekomendasi hukum yang tidak hanya normatif, tetapi juga kontekstual dan progresif.

HASIL DAN PEMBAHASAN

Implementasi Penegakan Undang-Undang ITE Terhadap Kasus *Cyber Deepfake* Bermuatan Video Hoax Di Indonesia

Dalam beberapa kepustakaan, tindak pidana mayantara atau *cyber crime* kerap dipersamakan dengan *computer crime*. Pengertian *cyber crime* secara general yaitu perbuatan yang dilakukan orang dengan komputer sebagai objek, dengan maksud untuk merugikan pihak lain (Maskun, S. 2022). Volodymyr Golubev menyebut tindak pidana mayantara sebagai bentuk baru dari perilaku anti sosial. Beberapa nama lain yang diberikan pada tindak pidana dunia maya sebagai tindak pidana dalam dimensi baru dari tindak pidana modern dan tindak pidana kerah putih (Ladito R. Bagaskoro et al.,2023).

Di dalam undang-undang ITE, istilah AI tidak disebutkan secara langsung, tetapi sifat-sifat AI dalam pengelolaan informasi memungkinkan untuk disebut sebagai "Agen Elektronik" berdasarkan hukum di Indonesia. Pada Pasal 1 UU ITE, "Agen Elektronik" didefinisikan sebagai "perangkat yang menjadi bagian

dari sistem elektronik yang dirancang untuk melaksanakan suatu tindakan secara otomatis terhadap informasi elektronik tertentu yang dikelola oleh manusia. " Kata "otomatis" dalam definisi "Agen Elektronik" berfungsi untuk mendefinisikan AI sebagai salah satu bentuk dari "Agen Elektronik". Dengan cara ini, regulasi yang ada tentang "Agen Elektronik" juga dapat diterapkan pada AI (Adnasohn Aqilla Respati, 2024).

Terdapat panduan etika dari Kementerian Komunikasi dan Digital RI (KOMDIGI) yang tercantum dalam Surat Edaran (SE) Nomor 9 Tahun 2023 mengenai Etika Kecerdasan Artifisial. Di sisi lain, Otoritas Jasa Keuangan (OJK) juga telah meluncurkan Panduan Kode Etik AI melalui kerja sama dengan Asosiasi Financial Technology Indonesia (AFTECH) dan sejumlah asosiasi industri lainnya, seperti AFSI (Asosiasi Fintech Syariah Indonesia), (Asosiasi Fintech Pendanaan Bersama Indonesia) AFPI, dan (Asosiasi Layanan Urun Dana Indonesia) ALUDI. Bersama-sama, mereka menyusun dan menetapkan Panduan Kode Etik Kecerdasan Buatan yang bertanggung jawab dan terpercaya di industri teknologi finansial, serta sedang merumuskan regulasi terkait layanan digital yang mencakup penggunaan AI. Menurut Pratama Persadha dalam Kiwantoro, terkait etika penggunaan AI saat ini masih bersifat imbauan dan tidak memiliki kekuatan hukum karena tidak mencantumkan sanksi terhadap pelaku usaha yang mengabaikannya (D. Dj. Kliwantoro 2025). Kriteria dalam pengaturan AI yang hanya tertuang pada peraturan di atas serta dalam beberapa pasal saja tidak cukup untuk mengatur AI secara keseluruhan, baik teknis maupun pelaksanaan dan penyelenggaraannya. Selain itu, berdasarkan penjelasan Hamdi selaku Penelaah Teknis Kebijakan pada Kementerian Komunikasi dan Digital (KOMDIGI), menyatakan bahwa Komdigi sudah melakukan edukasi dikalangan Masyarakat agar tidak mudah terkena dampak dari video *Hoax* berbasis *deepfake*.

Undang-Undang ITE mengatur mengenai tindak pidana penghinaan dan pencemaran nama baik secara elektronik, yakni melarang setiap individu untuk

mendistribusikan atau mentransmisikan konten yang mengandung unsur penghinaan atau pencemaran nama baik melalui media elektronik. Namun, seiring pesatnya perkembangan teknologi, terutama dengan hadirnya teknologi *deepfake*, ketentuan tersebut mulai menunjukkan keterbatasannya. Teknologi *deepfake* memungkinkan manipulasi wajah, suara, dan ekspresi seseorang dengan tingkat realisme tinggi sehingga menghasilkan konten yang tampak autentik padahal palsu. Sayangnya, karena belum diatur secara tegas, ketentuan dalam UU ITE sering kali tidak mampu menjangkau pelaku penyebaran konten *deepfake*, khususnya apabila konten tersebut tidak secara langsung menampilkan bentuk penghinaan verbal maupun tulisan, tetapi justru merusak citra atau reputasi seseorang melalui manipulasi visual.

Selain itu, kejahatan berbasis teknologi informasi atau *cybercrime* memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Dari sisi pelaku, *cybercrime* umumnya dilakukan oleh individu atau kelompok dengan kemampuan teknis tinggi yang memanfaatkan teknologi informasi, serta kerap beroperasi secara anonim melalui jaringan global sehingga identitasnya sulit dilacak. Korban kejahatan ini pun tidak terbatas pada individu di suatu wilayah tertentu, tetapi dapat mencakup masyarakat luas, perusahaan, bahkan negara, mengingat sifat ruang siber yang tidak mengenal batas geografis. Perbedaan yang signifikan juga terlihat pada modus operandi, di mana *cybercrime* dilakukan melalui perangkat digital, teknik peretasan, manipulasi data, pembuatan *deepfake*, atau penipuan berbasis internet, sehingga bukti yang dihasilkan bersifat elektronik, mudah diubah, disembunyikan, atau dihapus, dan membutuhkan keahlian serta alat forensik digital tertentu untuk pembuktiannya. Selain itu, tempat kejadian perkara dalam *cybercrime* tidak berada pada satu lokasi fisik tertentu, melainkan tersebar secara virtual melalui

server, perangkat, atau platform digital yang bahkan dapat berada di berbagai negara. Kondisi ini menimbulkan hambatan yurisdiksi dan membutuhkan pengaturan serta mekanisme penegakan hukum khusus di luar KUHP dan KUHAP untuk memberikan kepastian hukum dalam penanganan kasus *cybercrime*. Terkait dengan prinsip pembuktian hukum seringkali menimbulkan dilema, di satu sisi diharapkan agar hukum dapat beradaptasi dengan kemajuan zaman dan teknologi, sementara di sisi lain juga penting untuk adanya pengakuan hukum terhadap berbagai inovasi teknologi digital agar dapat berperan sebagai bukti di pengadilan.

Penerapan dan penegakan hukum terhadap tindak pidana siber menghadapi berbagai kendala, khususnya dalam proses penyelesaiannya. Karakter kejahatan siber yang bersifat *paperless* menimbulkan persoalan pembuktian terhadap informasi yang diproses, disimpan, atau dikirim secara elektronik, terutama karena belum adanya standar atau dasar hukum yang jelas mengenai penggunaan alat bukti elektronik dalam peraturan perundang undangan. Selain itu, kesulitan dalam mengidentifikasi pelaku serta membuktikan perbuatannya menjadikan tindak pidana siber sebagai tantangan tersendiri dalam praktik penegakan hukum.

Tindak pidana siber seperti *cyber deepfake, cyber porn, cyber terrorism, hacking*, dan sebagainya dapat terungkap baik melalui kegiatan patroli siber (*cyber patrol*) yang dilakukan oleh penyidik maupun melalui laporan korban. Umumnya, pelanggaran tersebut terdeteksi melalui layar komputer yang terhubung ke jaringan internet atau melalui penelusuran langsung di tempat umum seperti warung internet. Tahap awal penyelidikan biasanya melibatkan penggunaan perangkat elektronik seperti komputer, telepon genggam, tablet, serta jaringan internet yang saling terkoneksi. Bukti bukti kejahatan siber umumnya tersimpan dalam sistem elektronik atau perangkat digital tersebut. Meskipun Pasal 5 dan 6 UU ITE telah mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah dalam proses hukum, hingga kini belum

terdapat mekanisme atau ketentuan teknis yang secara jelas mengatur cara membedakan antara konten digital yang asli dan yang telah dimanipulasi, seperti *deepfake*. Kondisi ini menimbulkan tantangan serius dalam proses penegakan hukum, terutama pada tahap peradilan pidana, di mana autentikasi dan keabsahan alat bukti memiliki peran yang sangat krusial.

Penegakan hukum terhadap tindak pidana siber tidak hanya bertumpu pada keberadaan regulasi, tetapi juga harus didukung oleh peningkatan kapasitas aparat penegak hukum dalam menangani kejahatan siber. Perkembangan modus *cybercrime* yang semakin kompleks berpotensi menyebabkan kejahatan tersebut semakin meluas, sementara pelakunya sulit diidentifikasi dan ditangkap, sehingga dapat menimbulkan kerugian bagi masyarakat, negara, bahkan dunia luas. Teknologi *deepfake* mampu menghasilkan konten visual dan audio yang tampak sangat autentik, sehingga berpotensi dimanfaatkan sebagai alat bukti palsu dalam proses peradilan. Apabila keaslian konten tersebut tidak dapat diidentifikasi dan diverifikasi secara andal, kondisi ini dapat mengganggu prinsip *due process of law* (proses hukum yang adil) serta hak atas *fair trial* (persidangan yang jujur dan imparsial) (Sekaring Ayumeida Kusnadi et al., 2024). Penggunaan *deepfake* berpotensi menyesatkan hakim, penuntut umum, maupun penasihat hukum, yang pada akhirnya dapat melahirkan putusan yang tidak adil, baik berupa pemidanaan terhadap pihak yang tidak bersalah maupun pembebasan terhadap pelaku yang seharusnya dimintai pertanggungjawaban.

Seperti yang sudah dijelaskan, masih terdapat kendala dalam penerapan pasal-pasal ini dalam konteks *deepfake*, antara lain:

1. Tidak adanya definisi hukum terhadap *deepfake* membuat aparat penegak hukum kesulitan mengkualifikasikan tindakan pelaku dalam kerangka hukum positif yang sudah ada.

2. Sulitnya pembuktian bahwa pelaku memiliki niat jahat (*mens rea*) dalam menyebarkan konten *deepfake*, apalagi jika konten dibuat untuk parodi atau *satire*.
3. Minimnya kemampuan digital forensik di lembaga penegak hukum Indonesia dalam mengidentifikasi dan memverifikasi konten *deepfake* secara akurat.
4. Aspek lintas batas digital, yaitu banyaknya pelaku atau *platform* yang beroperasi di luar negeri, membuat proses hukum menjadi lebih kompleks karena yurisdiksi tidak jelas (Putri Ramadhani Rangkuti et al., 2025).

Seperti yang sudah disebutkan pada poin 1 sampai dengan 4 diatas, bahwa terdapat tantangan teknis dalam memahami teknologi AI juga menjadi kendala yang signifikan bagi penegak hukum. Teknologi AI sering kali melibatkan algoritma yang kompleks dan data dalam jumlah besar, yang memerlukan keahlian khusus untuk dianalisis. Banyak aparat penegak hukum, terutama di negara berkembang seperti Indonesia, tidak memiliki kapasitas teknis atau infrastruktur yang memadai untuk menyelidiki kejahatan berbasis AI. Sebagai contoh, dalam kasus *deepfake*, teknologi AI yang digunakan untuk memanipulasi video atau audio sehingga tampak autentik, penegak hukum memerlukan alat forensik digital yang canggih untuk mendeteksi manipulasi tersebut. Namun, alat dan keahlian ini sering kali tidak tersedia, sehingga menyulitkan proses investigasi dan penuntutan.

Dengan demikian, dapat diketahui bahwa berbagai kendala dalam proses penegakan Undang-Undang ITE terhadap kasus *cyber deepfake* bermuatan video *hoax* di Indonesia menunjukkan bahwa hukum positif yang berlaku saat ini masih belum sepenuhnya mampu menjawab kompleksitas perbuatan pidana yang berbasis kecerdasan buatan. Permasalahan ini tidak hanya menyangkut aspek substansi hukum, tetapi juga mencakup aspek struktur penegakan dan

budaya hukum masyarakat digital yang belum siap menghadapi perkembangan teknologi informasi secara menyeluruh.

Urgensi Reformulasi Pengaturan Hukum Undang-Undang ITE Terhadap Penyalahgunaan AI Yang Menggunakan *Cyber Deepfake* Sebagai Berita *Hoax*.

Hoax di Indonesia saat ini sangat marak dan banyak sekali dilakukan oleh masyarakat Indonesia untuk membuat orang lain mempercayai terhadap suatu kejadian. Adapun Kata *hoax* berasal dari "*hocus pocus*" yang aslinya adalah Bahasa latin "*hoc est corpus*" artinya "ini adalah tubuh". Kata ini biasa digunakan penyihir untuk mengklaim bahwa sesuatu adalah benar, padahal belum tentu benar (Ilham Nurfaizi Kurniawan et al.,2021).

Perkembangan teknologi yang pesat turut membawa berbagai konsekuensi, salah satunya munculnya beragam pola dan motif baru dalam kejahatan siber (Sekaring, 2025). Kekhawatiran terhadap kecerdasan buatan dan adanya kekosongan hukum bukanlah hal yang tanpa alasan. Sejumlah tokoh ternama seperti Stephen Hawking, Steve Wozniak, dan Elon Musk telah memperingatkan bahwa kemajuan AI berpotensi menjadi ancaman serius bagi umat manusia. Mereka menegaskan perlunya pengaturan baik di tingkat nasional maupun internasional untuk mengendalikan dampak yang ditimbulkan oleh teknologi tersebut. Sejalan dengan itu, pesatnya perkembangan AI di Indonesia menurut laporan *SEA e-Conomy* 2025 yang dirilis *Google*, Indonesia mendulang lonjakan pendapatan hingga 127 persen. Indonesia tercatatkan sebagai kedua tertinggi di Asia Tenggara dengan 80% penggunaan AI setiap hari (Adnasohn Aqilla Respati, 2024). Oleh karena itu, pemerintah Indonesia membutuhkan sebuah perangkat hukum yang siap memastikan peraturan atas penggunaan kecerdasan buatan yang aman dan etis. Indonesia tertinggal dalam regulasi AI meskipun memiliki visi AI untuk 2020 2045 dari Badan Pengkajian dan Penerapan Teknologi (BPPT).

Sampai saat ini, Indonesia belum memiliki peraturan khusus mengenai kecerdasan buatan (AI). Jika kita melihat negara-negara Uni Eropa yang saat ini

sedang menyusun peraturan pertama mengenai penggunaan AI, seperti dilaporkan oleh CNBC Indonesia dan VOA Indonesia, pejabat Uni Eropa saat ini sedang bernegosiasi untuk membahas peraturan terkait AI pada tanggal 14 Juni 2023. Tanpa peraturan khusus mengenai kecerdasan buatan (AI) di Indonesia, dampaknya dapat bervariasi terhadap masyarakat. Jika kita melihat upaya Uni Eropa untuk menyusun peraturan pertama mengenai penggunaan AI, seperti dilaporkan oleh CNBC Indonesia dan VOA Indonesia, dampaknya dapat dirasakan dalam beberapa cara :

a. Ketidakpastian Hukum

   Ketiadaan regulasi yang jelas mengenai penggunaan AI dapat menimbulkan ketidakpastian hukum di masyarakat. Individu, perusahaan, dan lembaga mungkin kesulitan memahami batasan hukum dan tanggung jawab mereka terkait penggunaan teknologi AI.

b. Risiko Terhadap Privasi Data

   Tanpa pedoman yang tepat, risiko terhadap privasi data pengguna dapat meningkat. Penggunaan AI dalam pengumpulan, analisis, dan pemrosesan data dapat memberikan peluang untuk pelanggaran privasi yang tidak diinginkan.

c. Perlindungan Konsumen yang Terbatas

   Ketiadaan regulasi dapat mengakibatkan perlindungan yang terbatas terhadap konsumen yang melakukan tindakan merugikan atau manipulatif yang melibatkan penggunaan AI. Hal ini dapat meningkatkan kerentanan konsumen terhadap penipuan atau eksploitasi.

d. Ketergantungan pada Teknologi Asing

   Tanpa regulasi yang kuat, masyarakat Indonesia mungkin menjadi lebih bergantung pada teknologi kecerdasan buatan (AI) dari luar negeri yang mungkin tidak sepenuhnya memperhitungkan nilai-nilai lokal, kepentingan nasional, atau kebutuhan masyarakat Indonesia (Salma Maulida Husana et al.,2024).

Kekosongan hukum dalam UU ITE, khususnya terkait regulasi penggunaan AI seperti teknologi *deepfake*, semakin menonjol dengan meningkatnya kasus penipuan digital. Data yang diperoleh dari PT Indonesia *Digital Identity* (VIDA) menunjukkan terjadinya lonjakan sebesar 1. 550% dalam kasus penipuan berbasis *deepfake* antara tahun 2022 dan 2023. Hal ini mengindikasikan adanya kelemahan dalam kerangka hukum kita dalam mengantisipasi dan menangani ancaman yang muncul. Teknologi *deepfake* tidak hanya berpotensi untuk mencuri identitas dan memalsukan dokumen, tetapi juga meningkatkan risiko terhadap keamanan transaksi digital. Saat ini, solusi teknologi seperti *VIDA Identity Stack* (VIS) dan *VIDA Sign* telah dikembangkan untuk menghadapi ancaman ini. Namun, regulasi yang mendukung penerapan teknologi tersebut secara menyeluruh masih sangat minim. (Iskandar, 2025)

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), meskipun telah mengalami pembaruan sejak pengesahannya pada tahun 2008, masih dianggap kurang memadai dalam menangani risiko yang ditimbulkan oleh penggunaan kecerdasan buatan, termasuk teknologi *deepfake*. Terdapat beberapa alasan utama yang menjadikan UU ITE dianggap tidak efektif dalam menghadapi masalah ini. Undang-Undang ITE tidak memberikan definisi yang jelas mengenai "*deepfake*" atau teknologi AI lainnya, sehingga menyulitkan penerapan hukum terhadap praktik-praktik tersebut. Selain itu, UU ITE lebih menekankan pada regulasi umum mengenai informasi dan transaksi elektronik tanpa mencakup isu-isu spesifik yang berkaitan dengan teknologi AI, seperti manipulasi media dan penyebaran informasi yang salah.

Pada Kasus Presiden Prabowo, kasus Gubernur Jawa Timur Khofifah Indar Parawansa, dan kasus *deepfake porn* mahasiswa unud, dari kasus ini dapat diketahui bahwasanya teknologi kecerdasan buatan berbasis deepfake menjadi tantangan dalam pembuktian, hal itu terjadi karena, Teknologi deepfake mampu menghasilkan video yang sangat realistis sehingga menyulitkan proses pembuktian forensik. Selain itu, untuk membuktikan bahwa sebuah video

merupakan hasil *deepfake*, diperlukan analisis *metadata, pixel mapping*, dan AI *forensic tools*, yang belum dimiliki secara merata oleh aparat penegak hukum. Selain itu, biasanya pelaku menggunakan akun anonim, menyulitkan pelacakan identitas. Hal ini tentunya membuat penegakan hukum terkait pelanggaran yang berkaitan dengan *deepfake* juga menjadi sulit, mengingat pengumpulan dan analisis bukti digital sering kali sangat kompleks. Sayangnya, UU ITE tidak menyediakan petunjuk yang memadai dalam hal ini. Di samping itu, Undang-Undang ini juga tidak mengatur ketentuan mengenai etika penggunaan AI, yang mencakup tanggung jawab para pengembang dan pengguna teknologi *deepfake*. Hal ini sangat penting untuk mencegah penyalahgunaan teknologi serta melindungi individu. Meskipun telah ditetapkannya Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, dan UU ITE No.1 tahun 2024 belum mengatur integrasi proteksi data dalam konteks penggunaan teknologi AI seperti *deepfake*, yang berpotensi melibatkan pemrosesan data pribadi tanpa izin.

Hukum pidana dianggap mengalami kegagalan dalam menangani tindak pidana yang dilakukan oleh *artificial intelligence*. Hal ini dikarenakan minimnya aturan pidana terkait dengan *artificial intelligence*, meskipun bahaya dari *artificial intelligence* telah dirasakan oleh masyarakat dunia. Sekretaris Jenderal PBB Antonio Guterres bahkan mengatakan bahwa *artificial intelligence* menimbulkan ancaman bagi umat manusia setara dengan “perang nuklir”. Sudah sepatutnya hukum hadir untuk melindungi masyarakat, khususnya masyarakat Indonesia. Tindak pidana yang timbul atas *artificial intelligence* seperti penyalahgunaan *deepfake* pada hakikatnya merupakan tindak pidana yang telah ada namun terpengaruh perkembangan teknologi. Seperti tindak pidana penipuan yang telah terdapat dalam KUHP, namun dengan hadirnya teknologi *deepfake* yang menggunakan identitas orang lain menjadikannya tindak pidana baru. Hal ini dikarenakan penyalahgunaan *deepfake* memiliki dampak yang lebih besar dari penipuan biasa (Chiquita Thefirstly Noerman,2024).

Kasus Penyalahgunaan *deepfake* yang melibatkan petinggi negara seperti Presiden Prabowo, Mantan mentri keuangan Sri Mulyani dan Gubernur Jawa Timur Khofifah Indar Parawansa. Memakan banyak nya korban yang terperdaya oleh video *hoax* berbasis *deepfake*, hal ini menandakan *deepfake* menjadi instrumen kejahatan yang menyasar kerentanan sosial ekonomi. Di samping kerugian materiil, ada potensi rusaknya kepercayaan masyarakat terhadap pemerintahan, maupun pejabat publik, hal itu dapat terjadi karena jika ada program bantuan pemerintah, masyarakat mulai tidak tahu mana yang benar, hal ini dapat menyebabkan kerusakan sosial bisa melebar. Tidak hanya menggunakan aspek verbal dalam penipuan, namun juga aspek visual yang menggunakan identitas orang lain. Aspek visual memiliki efek yang lebih besar dikarenakan secara umum manusia lebih mengandalkan informasi secara visual dibandingkan informasi sensorik lainnya yang disebut sebagai efek dominasi visual colavita. Efek dominasi visual colavita menjelaskan bahwa masyarakat lebih cenderung mengingat pesan visual daripada pesan verbal, yang menyebabkan informasi visual palsu lebih banyak dipercaya dibandingkan dengan informasi verbal.

Hadirnya tindak pidana atas penyalahgunaan *deepfake* seharusnya dapat diatasi dengan penerapan hukum. Namun dengan tidak adanya aturan di Indonesia yang mengatur mengenai *deepfake* secara eksplisit dapat menyebabkan kekosongan hukum yang menimbulkan ketidakpastian hukum. Hal ini dikarenakan ketidakjelasan mengenai apa yang harus dilakukan untuk mencegah maupun menanggulangi tindak pidana *deepfake* maupun tindak pidana yang akan datang dari sebuah *artificial intelligence*. Kekosongan hukum ini dengan jelas menggambarkan adagium *het recht hinkt achter de faiten aan* yang menyatakan bahwa hukum diibaratkan berjalan tertatih-tatih yang mana tertinggal dari perkembangan manusia.

Dengan demikian, dapat diketahui bahwa berbagai permasalahan yang telah diuraikan sebelumnya menunjukkan adanya kesenjangan antara

perkembangan teknologi kecerdasan buatan, khususnya fenomena *cyber deepfake*, dengan pengaturan hukum pidana yang diatur dalam Undang-Undang ITE saat ini. Kesenjangan tersebut pada akhirnya menjadi hambatan dalam proses penanggulangan penyalahgunaan teknologi AI, terutama ketika *deepfake* digunakan untuk membuat dan menyebarkan berita bohong yang dapat menimbulkan keresahan, fitnah, bahkan gangguan stabilitas sosial dan politik di masyarakat. Berbagai kendala tersebut juga pada akhirnya akan dapat diselesaikan atau tidaknya sangat bergantung pada profesionalitas pemerintah, pembuat kebijakan, serta aparat penegak hukum dalam menerapkan hukum secara adaptif dan progresif terhadap bentuk kejahatan baru berbasis teknologi. Jika penegakan hukum hanya dilakukan secara tekstual tanpa adanya

Pengaturan Deepfake Di Beberapa Negara

Pengaturan *deepfake* di Uni Eropa

Uni Eropa telah mengesahkan pembaruan terbaru *EU AI Act Regulation* yang menitikberatkan pada pendekatan berbasis manajemen risiko dalam penggunaan kecerdasan buatan dan mulai berlaku pada tahun 2024. Kebijakan ini dapat dijadikan rujukan penting dalam upaya reformulasi Undang-Undang ITE guna mengatasi berbagai keterbatasan pengaturan hukum yang ada, meskipun regulasi tersebut menuai kritik dari sejumlah perusahaan teknologi besar karena dinilai memiliki tingkat kompleksitas kepatuhan yang tinggi (Adnasohn Aqilla Respati,2024). Peraturan tersebut mengatasnamakan Uni Eropa, akan tetapi tidak semua negara di Uni Eropa sepenuhnya terikat pada peraturan *EU AI Act*, meskipun undang-undang tersebut telah disetujui oleh seluruh anggota Dewan dan Parlemen Eropa.

Dalam pengaturan *deepfake*, reformulasi UU ITE perlu mengadopsi prinsip-prinsip kunci dari *EU AI Act Regulation*. Pengaturan tersebut mencakup perumusan definisi teknis *deepfake* sebagaimana diatur dalam *Article* 3 ayat (60), selain itu, perlu penerapan prinsip transparansi melalui kewajiban

pelabelan dan *watermarking* pada konten sintetis, serta pengklasifikasian sistem AI berisiko tinggi sesuai dengan *Recitals* 132–137. Selain itu, UU ITE perlu mengatur mekanisme pelaporan publik atas penyalahgunaan *deepfake* dan menetapkan sanksi yang tegas dan proporsional, termasuk denda maksimum hingga *EUR 35 million* atau 7% dari pendapatan tahunan global sebagaimana diatur dalam *Article* 99 ayat (3) EU AI Act, serta mendorong kerja sama internasional dengan Uni Eropa guna mewujudkan harmonisasi regulasi kecerdasan buatan.

EU AI Act mengatur aspek-aspek penting penggunaan AI yang belum diakomodasi dalam UU ITE Indonesia, khususnya terkait AI berisiko tinggi dan berisiko tidak dapat diterima. Regulasi ini bertujuan menjamin pemanfaatan AI yang aman, transparan, non-diskriminatif, serta melindungi hak asasi manusia. Ketentuan yang belum diatur dalam UU ITE meliputi larangan manipulasi perilaku kognitif manusia, praktik *social scoring* yang merugikan, penggunaan pengenalan biometrik yang melanggar privasi, pengaturan sistem AI berisiko tinggi, kewajiban pendaftaran penyedia AI, uji kesesuaian terhadap standar keamanan dan transparansi, serta mekanisme pengawasan dan mitigasi bias oleh otoritas berwenang.

Pengaturan *deepfake* di china

Selain Uni Eropa, China juga memiliki regulasi AI yang sejalan melalui kebijakan *Generative AI Measures*. Cyberspace Administration of China* (CAC) mengatur pelabelan konten sintetis berbasis AI untuk menjaga keamanan nasional dan kepentingan publik. Terkait deepfake, China menerapkan *Provisions on the Administration of Deep Synthesis of Internet-based Information Services* yang menitikberatkan pada pengelolaan risiko dan pencegahan penyalahgunaan. Melalui pengaturan komprehensif atas *AI generatif*, algoritma rekomendasi, dan inovasi AI, China bersama Uni Eropa

menunjukkan pendekatan berbeda namun sama-sama serius dalam membangun tata kelola AI yang kuat.

Pengaturan teknologi deepfake di China diatur dalam *Provisions on the Administration of Deep Synthesis of Internet-based Information Services* yang mulai berlaku pada 10 Januari 2023. Regulasi ini bertujuan untuk mengendalikan dan mengawasi pemanfaatan teknologi *deep synthesis*, yaitu teknologi berbasis algoritma generatif seperti *deep learning* dan realitas virtual yang digunakan untuk mencipta atau memodifikasi konten berupa teks, gambar, suara, dan video, yang berpotensi disalahgunakan. Dalam ketentuan tersebut, penyelenggara layanan diwajibkan melakukan verifikasi identitas pengguna, memperoleh persetujuan atas penggunaan dan pengolahan data, memberikan penandaan terhadap konten hasil sintesis, serta melakukan penyaringan terhadap informasi yang melanggar hukum. Selain itu, penyedia layanan juga berkewajiban menjamin perlindungan data pribadi dan menerapkan mekanisme pengamanan terhadap data yang digunakan dalam proses pelatihan sistem. Pemerintah diberikan kewenangan untuk melakukan penegakan hukum dan menjatuhkan sanksi atas pelanggaran, sehingga regulasi ini mencerminkan langkah strategis China dalam mendorong transparansi, akuntabilitas, serta pencegahan penyalahgunaan teknologi yang berpotensi mengancam keamanan nasional.

KESIMPULAN DAN SARAN

Perkembangan teknologi kecerdasan buatan, khususnya deepfake, telah menimbulkan tantangan serius bagi penegakan hukum pidana di Indonesia karena karakter manipulasi audio-visualnya yang realistis, lintas batas, dan sulit dibuktikan secara forensik. Pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik masih bersifat umum dan belum secara eksplisit mengakomodasi risiko serta karakteristik khusus deepfake, sehingga menimbulkan ketidakpastian hukum, kelemahan pembuktian, dan hambatan dalam penentuan pertanggungjawaban pidana. Kondisi ini menunjukkan adanya

kesenjangan antara perkembangan teknologi dan norma hukum yang berlaku, yang berpotensi melemahkan perlindungan masyarakat di ruang digital. Oleh karena itu, reformulasi UU ITE menjadi kebutuhan mendesak dalam kerangka pembaharuan hukum pidana nasional dengan menegaskan definisi hukum deepfake, memperjelas larangan dan sanksi pidana, serta mengintegrasikan mekanisme preventif seperti kewajiban transparansi, pelabelan konten sintetis, dan penguatan tanggung jawab platform digital. Selain pendekatan penal, pemerintah juga perlu mengembangkan kebijakan non-penal melalui peningkatan literasi digital dan kapasitas aparat penegak hukum di bidang forensik digital, agar sistem hukum nasional mampu beradaptasi secara efektif, proporsional, dan berkeadilan terhadap perkembangan teknologi kecerdasan buatan.

DAFTAR REFERENSI

Adnasohn Aqilla Respati (2024). Analisis Hukum terhadap Pencegahan Kasus *Deepfake* serta Perlindungan Hukum terhadap Korban, *Media Hukum Indonesia* 2(2), 587, https://doi.org/10.5281/zenodo.12508126.

Adnasohn Aqilla Respati (2024). Reformulasi Undang-Undang ITE terhadap *Artificial Intelligence* Dibandingkan dengan Uni Eropa dan China *AI Act Regulation. USM Law Review,* 7(3),1748, https://doi.org/10.26623/julr. v7i3.10578.

Andhika Nugraha Utama, Prama Tusta Kesuma, dan Rio Maulana Hidayat, (2023). Analisis Hukum terhadap Upaya Pencegahan Kasus *Deepfake Porn* dan Pendidikan Kesadaran Publik di Lingkungan Digital, *Jurnal Pendidikan Tambusai* 7(3), 26180, https://doi.org/10.31004/jptam.v7i3.10815.

Chiquita Thefirstly Noerman, Lukman Ibrahim. (2024). Kriminalisasi Deepfake di Indonesia sebagai Bentuk Pelindungan Negara. *Jurnal USM Law Review*, 7(2), 604. https://doi.org/10.26623/julr.v7i2.

D. Dj. Kliwantoro. (2024). Regulasi AI Sudah Cukup, Tinggal Penegakan Hukum Berkeadilan. Antara News, https://www.antaranews.com/berita/4467965/ regulasi-ai-sudah-cukup-tinggal-penegakan hukum-berkeadilan, diakses 24 Januari 2025.

Hendra, Jaya, dkk. (2018). *Kecerdasan Buatan. Makassar*: Fakultas MIPA Universitas Negeri Makassar.

Ilham Nurfaizi Kurniawan, benny irawan, Rena Yulia. (2021). Tinjauan

Kriminologis Terhadap Pelaku Tindak Pidana Penyebaran Hoax Kasus Sunda Empire. *Yustisia Tirtayasa. Jurnal Tugas Akhir,* 1(2), 23-34. http://dx.doi.org/10.51825/yta.v1i2.12053

Iskandar. (2025). Modus Penipuan Deepfake Naik 1.550 Persen di Indonesia." Liputan6. https://www.liputan6.com/tekno/read/5769565/moduspenipuan deepfake-naik-1550-persen-di-indonesia?page=4, Diakses 20 Januari 2025.

Ladito R. Bagaskoro et al.,(2023). *Perkembangan Hukum Pidana Di Indonesia.* Sada Kurnia Pustaka.

Putri Ramadhani Rangkuti, Rahma Fitri Amelia Hasibuan, dkk. (2025). Analisis Yuridis terhadap Penggunaan *Deepfake* dalam Pelanggaran UU ITE: Studi Kasus di Media Sosial Indonesia," Deposisi. *Jurnal Publikasi Ilmu Hukum*.3(2),116. https://doi.org/10.59581/deposisi.v3i2.5080.

Riswandi, dan B. Agus. (2006). *Hukum Cyberpace* Yogyakarta: Gita Nagari.

Salma Maulida Husana, Farid Hibatullah, dan Muhamad Romdoni. (2024). Limiting The Use Of Ai By Creating Regulations That Can Prevent The Occurring Of Digital Crime, *International Journal of Law Society Services,* 4(1). https://dx.doi.org/10.26532/ijlss.v4i1.37795

Sekaring Ayumeida Kusnadi dan Dina Wanda Setiawan Putri. (2025). Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi *Deepfake* di Indonesia, *Jurnal Rechts Vinding*, 14(2), 196, https://doi.org/10.33331 /rechtsvinding.v14i2.2135.

Wahyudi, BR. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *INNOVATIVE, Journal of Social Science Research,* 5(1). https://doi.org/10.31004/innovative.v5i1.17519.