JURNAL HUKUM SEHASEN
p-ISSN : 2528-5025
e-ISSN : 2746-6485

Comparative Study: The Urgency Of Reformulating Deepfake Criminal Sanctions In The Criminal Code And The ITE Law

Studi Komparatif: Urgensi Reformulasi Sanksi Pidana Deepfake Dalam Kuhp Dan UU ITE

Muhammad Ijzlal Ramadan [1]; Endik Wahyudi [2]
[1,2] Universitas Esa Unggul
Email: [1] *ijzlalramadan@student.esaunggul.ac.id* ;[2] endik.wahyudi@esaunggul.ac.id

ARTICLE HISTORY
Received [22 Juli 2025]
Revised [01 Oktober 2025]
Accepted [06 Oktober 2025]

KEYWORDS
Deepfake, Komparatif, Regulasi.

ABSTRAK
Penelitian ini membahas urgensi reformulasi sanksi pidana terhadap kejahatan digital berupa *deepfake* dalam perspektif hukum Indonesia, khususnya dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP). Fokus utama penelitian ini adalah menganalisis pengaturan hukum positif di Indonesia serta melakukan perbandingan dengan regulasi di Korea Selatan dan Amerika Serikat. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan hukum. Hasil penelitian menunjukkan bahwa Indonesia belum memiliki pengaturan khusus mengenai *deepfake*, sementara beberapa negara telah menerapkan regulasi yang lebih adaptif. Oleh karena itu, dibutuhkan pembaruan hukum yang komprehensif guna mengantisipasi dampak negatif teknologi kecerdasan buatan terhadap hak privasi, integritas demokrasi, dan ketertiban sosial.

ABSTRACT
This research examines the urgency of reformulating criminal sanctions for digital crimes involving deepfake technology within the framework of Indonesian law, particularly the Law on Electronic Information and Transactions (UU ITE) and the Indonesian Penal Code (KUHP). The primary focus is to analyze the current legal framework in Indonesia and compare it with regulations in South Korea and the United States. This study employs a normative juridical method with a statutory, conceptual, and comparative approach. The findings reveal that Indonesia does not yet have specific provisions regulating deepfake, whereas several countries have enacted more adaptive legal instruments. Therefore, comprehensive legal reform is necessary to anticipate the negative impacts of artificial intelligence technologies on privacy rights, democratic integrity, and public order.

PENDAHULUAN

Inovasi teknologi informasi yang berkembang pesat memungkinkan membuka peluang bagi manusia untuk beraktivitas di luar dunia fisik, namun memberikan fasilitas untuk menjalankan aktivitas daring secara virtual. Situasi ini membuka akses bagi manusia untuk melakukan berbagai kegiatan di dunia digital. Oleh karena itu, sebagaimana di kehidupan nyata, perilaku manusia dalam dunia maya turut membentuk dinamika sosial tersendiri (*cyber space*) seyogianya tidak terlepas dari kontrol dan regulasi yang ditetapkan oleh hukum.

Pendayagunaan teknologi informasi digunakan untuk menunjang kegiatan di ruang digital Hakikatnya aktivitas ini bersumber dai manusia dan harus tetap dikaitkan dengan realitas kehidupannya secara fisik(Budhijanto Danrivanto, 2025). Perkembangan teknologi yang pesat ini semakin mempermudah aktivitas manusia seperti interaksi sosial, tetapi juga memunculkan beraneka ragam konten digital dengan kualitas visual interaktif yang inovatif. Salah satu wujud nyata kemajuan teknologi yang kini menjadi perhatian publik adalah pemunculan *deepfake. Deepfake* adalah teknik yang memanfaatkan AI untuk membuat, mengga bungkan, atau memodifikasi gambar, video, atau audio sehingga tampak seperti asli, padahal merupakan hasil rekayasa.

Kemampuan *deepfake* untuk meniru wajah dan suara individu dengan sangat meyakinkan telah menimbulkan kekhawatiran terkait penyalah gunaannya dalam berbagai bentuk kejahatan siber, seperti pengelabuhan , tuduhan yang tidak benar, dan berita bohong(Shevila Kristiyenda et al., 2025). Di Indonesia, pemanfaatan teknologi *deepfake* telah di temukan dalam berbagai bentuk, mulai dari pembuatan video humor, parodi, hingga penyebaran hoaks yang menyerang tokoh masyarakat, selebritas, maupun individu biasa.

Namun demikian, penyalahgunaan teknologi ini dalam pembuatan konten pornografi non-konsensual menjadi perhatian yang lebih serius. Menurut publikasi Databoks tahun 2023, Indonesia menempati peringkat ketiga global dalam penggunaan AI dengan 1,4 miliar kunjungan aplikasi AI, menyumbang 5,6% dari total traffic dunia (Fauzyah et al., 2024)

Dalam sejumlah kasus, wajah korban direkayasa dan disisipkan ke dalam video asusila, kemudian disebarluaskan kepada publik, sehingga menimbulkan dampak kerugian sosial serta trauma psikologis yang mendalam bagi korban. Salah satu kasus terbaru di Indonesia yang memanfaatkan *deepfake* sebagai sindikatnya terjadi pada 16 Januari 2025 lalu dimana Bareskrim Polri berhasil menangkap penipuan dengan bantuan AI *deepfake* meng gunakan wajah presiden Prabowo Subianto dan penjabat lainnya di Lampung hingga meraup keuntungan mencapai Rp 30 juta dari 11 korban .

Kasus lainnya pernah pernah terjadi pada tahun 2023, dimana video *deepfake* menggunakan wajah mantan presiden Jokowi yang sedang memberikan pidato fasih menggunakan bahasa mandarin tersebar luas dikalangan masyarakat. Tidak hanya itu,beberapa pemalsuan kontem intim dengan AI *(revenge porn* berbasis *deepfake*), kasus *deepfake* pornografi turut melibatkan selebritas ternama, termasuk Syahrini dan Nagita Slavina termasuk kasus, dan banyak kasus lainnya yang juga menyerang masyarakat biasa(Latifatunnisa & Yudha Wira, 2025).

Pada dasarnya *deepfake* ini tak terlepas dari suatu isu kekerasan gender berbasis online (KGBO). Data Komisi Nasional (Komnas) pada tahun 2019 tercatat adanya 241 kasus,sedangkan di tahun 2020 mengalami suatu peningkatan menjadi 940 kasus(Putra Wicaksana & Dewi Prima Arya, 2024).Video hasil manipulasi AI ini memiliki detail begitu halus sehingga hampir tak terbantahkan keasliannya. Data golbal menunjukan peningkatan signifikan penggunaan *deepfake*, dari 7.964 kasus (2018) melonjak menjadi 14.678 kasus (2019), dengan 96% berupa konten pornografi(Amanda et al., 2024)

Hal ini menimbulkan pertanyaan besar: apakah sistem hukum Indonesia mampu merespons tantangan ini secara memadai?. Padahal melindungi data pribadi berarti melindungi hak dasar manusia atas kehidupan pribadinya oleh karena itu, perlindungan terhadap data pribadi membutuhkan dasar hukum yang sejalan dengan prinsip-prinsip konstitusi dalam UUD 1945. Upaya negara dalam melindungi data pribadi bertujuan untuk menjamin perlindungan terhadap hak-hak individu atas data dan meningkatkan kesadaran public dan memastikan pengakuan serta penghormatan terhadap urgensi perlindungan data pribadi.

Namun kondisi legislasi regulasi data pribadi saat ini masih diatur dalam berbagai ketentuan perundang-undangan. Untuk mewujudkan perlindungan data pribadi yang efektif diperlukan Langkah konkret dalam pratiknya yang menyeluruh dalam satu regulasi(Budhijanto Danrivanto, 2023). Hingga saat ini regulasi mengenai teknologi *deepfake* di Indonesia tidak terlalu fleksibel dalam menangani dampak buruk *deepfake*, dikarenakan belum secara spesifik memiliki undang-undang yang mengatur terkait dengan AI dan deepfake.

Meskipun beberapa ketentuan dalam KUHP dan UU Pornografi dapat dikenakan terhadap penyalah gunaan *deepfake*, seperti pasal terkait pencabulan atau penyebaran konten asusila, namun regulasi tersebut belum mengatur secara jelas mengenai penggunaan teknologi AI dan manipulasi digital sebagai metode kejahatan. Hal ini menunjukkan adanya kekosongan hukum yang bersifat substantif dalam menanggapi fenomena *deepfake* di Indonesia.

Para pelaku kejahatan digital seperti pembuat *deepfake* hanya dapat dijerat melalui pasal-pasal umum UU No 19 Tahun 2016 tentang (UU ITE), terutama Pasal 27 ayat (3) tentang penghinaan atau pencemaran nama baik, dan Pasal 28 ayat (1) mengenai penyebaran berita bohong. Selain itu, ketentuan pidana hukum yang berlaku, dalam KUHP juga digunakan, namun sifatnya masih sangat umum. PP No 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) juga belum secara eksplisit mengatur tentang konten *deepfake*. Bahkan dalam lingkup perlindungan data pribadi, UU No 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) belum menyebutkan secara eksplisit pelanggaran melalui media manipulatif seperti *deepfake.*

Penulis mengamati bahwa, regulasi terkait perbuatan *deepfake* di Indonesia belum diatur secara jelas dan belum mampu mengimbangi pesatnya perkembangan teknologi digital. Untuk itu, penulis perlu mengacu dibeberapa negara yang telah yang mengatur perbuatan deepfake,diantaranya Korea Selatan dan Amerika Serikat sebagai bahan analisis dan rujukan normatif bagi reformulasi hukum nasional.

Korea Selatan telah mengatur tindak pidana terkait deepfake dalam konteks pemilu melalui revisi *Public Officials Elections Act* (undang-undang Korean) pada Desember 2023. **Pasal 82-8** melarang produksi, penyebaran, dan penayangan konten *deepfake* selama 90 hari sebelum pemilu, dapat dikenakan hukuman hingga 7 tahun kurungan atau denda sebesar 10-50 juta won. Peraturan ini menunjukkan pendekatan hukum yang ketat dalam mencegah manipulasi konten digital berbasis AI demi menjaga integritas pemilu (Schuldt, 2024).

Selain itu di Korea Selatan Anggota parlemen Korea Selatan meloloskan rancangan undang-undang yang mengkriminalisasi kepemilikan atau menonton gambar dan video *deepfake* yang eksplisit seksual, dengan hukuman yang ditetapkan mencakup hukuman penjara dan denda. Siapa pun yang membeli, menyimpan, atau menonton materi tersebut terancam hukuman penjara selama 3 tahun atau pidana denda sebesar-besarnya 30 juta won ($22.600), menurut RUU tersebut. hukuman maksimum untuk kejahatan tersebut juga akan meningkat menjadi tujuh tahun, terlepas dari niatnya. Polisi Korea

Selatan sejauh ini telah menangani lebih dari 800 kasus kejahatan seks *deepfake* tahun ini,Jumlah tersebut lebih rendah dibandingkan dengan 156 kasus sepanjang tahun 2021, saat data pertama kali dikumpulkan. Sebagian besar korban dan pelaku adalah remaja, kata polis(Hyunsu, 2024).

Semantara itu, Regulasi tentang teknologi *deepfake* di negara Amerika, Dalam langkah bipartisan yang langka , Dewan Perwakilan Rakyat AS meloloskan Undang-Undang *Take It Down* dengan perolehan suara 409-2 pada tanggal 28 April 2025. RUU tersebut merupakan upaya untuk menghadapi salah satu penyalahgunaan internet yang paling mengerikan: penyebaran viral gambar seksual nonkonsensual, termasuk pornografi *deepfake* buatan AI dan foto asli yang dibagikan sebagai balas dendam porno. Undang-Undang *Take It Down* menargetkan "penggambaran visual intim tanpa persetujuan" - istilah hukum yang mencakup apa yang oleh kebanyakan orang disebut sebagai *revenge porn* dan *deepfake porn*. Ini adalah gambar atau video seksual, yang sering kali dimanipulasi secara digital atau sepenuhnya dibuat-buat, yang disebarkan secara daring tanpa persetujuan orang yang digambarkan.

RUU tersebut mewajibkan platform daring untuk membangun proses penghapusan yang mudah digunakan. Saat korban mengajukan permintaan yang sah, platform harus bertindak dalam waktu 48 jam. Kegagalan untuk melakukannya dapat memicu penegakan hukum oleh Komisi Perdagangan Federal, yang dapat memper lakukan pelanggaran tersebut sebagai penyalah gunaan wewenang.

Hukuman pidana juga berlaku bagi mereka yang menerbitkan gambar: Pelanggar dapat didenda dan menghadapi hukuman penjara hingga 3 tahun jika ada pelaku di bawah umur (kurang dari 18 tahun) dapat dihukum maksimal 2 tahun, sedangkan pelaku dewasa menghadapi hukuman hingga 5 tahun penjara(Lu, 2025).

Presiden Donald Trump menandatangani undang-undang pada hari Senin, 19 Mei 2025 yang mengkriminalisasi penyebaran gambar intim tanpa persetujuan, termasuk deepfake buatan AI dan *revenge porn*. "Hari ini, melalui Undang-Undang *Take It Down*, kami menegaskan bahwa kesejahteraan anak-anak kita adalah hal yang utama bagi masa depan keluarga kita dan Amerika," kata Melania Trump dalam upacara tersebut(Chatterjee, 2025).

Maka dari itu Indonesia dapat mengadopsi prinsip-prinsip dari negara tersebut untuk memperkuat sistem hukum pidana nasional dalam menghadapi tantangan kejahatan digital seperti *deepfake*. Indonesia dapat mengadopsi prinsip-prinsip dari negara tersebut untuk memperkuat sistem hukum pidana nasional dalam menghadapi tantangan kejahatan digital seperti *deepfake.*

LANDASAN TEORI

Penelitian ini mengandalkan beberapa landasan teori yang relevan untuk membangun pemahaman mengenai fenomena deepfake dan sanksi pidana yang dapat diterapkan. Landasan teori ini akan membahas prinsip-prinsip hukum pidana, teori tentang teknologi informasi dan kejahatan siber, serta teori hukum internasional yang berfungsi untuk menganalisis fenomena deepfake dalam konteks Indonesia dan negara lain.

Teori Hukum Pidana

Teori hukum pidana berperan dalam memberikan kerangka kerja untuk mengatur pelanggaran hukum yang dilakukan oleh individu atau kelompok dalam masyarakat. Hukum pidana bertujuan untuk memberikan sanksi terhadap perbuatan yang membahayakan ketertiban umum atau merugikan individu atau negara.

Dalam konteks kejahatan deepfake, teori hukum pidana memberikan dasar untuk menganalisis penerapan pasal-pasal yang ada dalam KUHP dan UU ITE terhadap kejahatan digital. Teori Sanksi Pidana (Punishement Theory) oleh Immanuel Kant yang menekankan pada keadilan retributif, di mana sanksi diberikan sebagai bentuk pembalasan atas pelanggaran yang dilakukan.

Dalam hal deepfake, sanksi pidana bertujuan untuk menegakkan keadilan bagi korban yang dirugikan oleh manipulasi konten digital. Selain itu, Teori Pemidanaan oleh Cesare Beccaria menekankan pentingnya kejelasan dan kepastian dalam penerapan hukuman. Dalam konteks deepfake, hal ini berarti pentingnya pembentukan regulasi yang jelas dan tegas agar pelaku kejahatan dapat dihukum secara adil dan transparan.

Teori Kejahatan Siber

Kejahatan Siber atau Cybercrime mengacu pada kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan internet sebagai sarana untuk melakukan perbuatan melawan hukum. Menurut Schneier (2000), kejahatan siber dapat mencakup penyebaran malware, penipuan online, pencurian data pribadi, hingga manipulasi media digital seperti dalam kasus deepfake. Teori Kejahatan Digital yang

dikembangkan oleh McGuire dan Dowling (2013) menyebutkan bahwa perkembangan teknologi telah mempercepat kemunculan kejahatan baru yang lebih sulit dideteksi dan ditangani oleh hukum konvensional.

Deepfake sebagai bentuk kejahatan digital ini menjadi salah satu contoh nyata di mana teknologi digunakan untuk tujuan merugikan orang lain, seperti penyebaran pornografi non-konsensual dan penipuan daring. Kejahatan siber juga mengingatkan pentingnya perubahan dalam regulasi hukum agar dapat merespons fenomena baru ini dengan tepat.

Teori Perlindungan Data Pribadi

Dalam konteks deepfake, perlindungan data pribadi menjadi isu penting, mengingat teknologi ini dapat dengan mudah memanipulasi identitas visual dan audio seseorang tanpa izin. Teori Perlindungan Data Pribadi yang dikembangkan oleh Alan Westin (1967), mengemukakan bahwa hak atas privasi dan perlindungan data pribadi merupakan hak dasar manusia yang harus dijamin oleh negara.

Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia bertujuan untuk melindungi hak-hak individu atas data pribadinya. Namun, dalam praktiknya, banyak regulasi yang belum sepenuhnya mengakomodasi ancaman baru seperti deepfake. Oleh karena itu, teori ini memberikan dasar untuk mendorong pembaruan regulasi yang lebih komprehensif terkait teknologi deepfake dalam sistem hukum Indonesia.

Teori Hukum Internasional

Teori Hukum Internasional mengatur hubungan antara negara-negara dalam hal perjanjian dan konvensi yang mengatur hak asasi manusia, perlindungan data, serta kejahatan siber. Dalam hal deepfake, beberapa instrumen internasional seperti Konvensi Cybercrime Council of Europe (2001) dan General Data Protection Regulation (GDPR) di Eropa memberikan dasar untuk mengatur kejahatan siber dan perlindungan data pribadi secara lebih ketat.

Konvensi Cybercrime mengatur perlindungan terhadap data pribadi dan pengaturan terkait dengan manipulasi media, termasuk penggunaan teknologi seperti deepfake. GDPR, yang diterapkan di Eropa, juga berfokus pada perlindungan data pribadi yang dapat digunakan untuk mengatasi penyalahgunaan teknologi deepfake yang merugikan individu.

Teori Perbandingan Hukum

Teori perbandingan hukum digunakan untuk menganalisis regulasi yang diterapkan di negara lain, dan kemudian membandingkannya dengan sistem hukum yang ada di Indonesia. Dalam hal ini, perbandingan hukum antara Indonesia dengan negara-negara seperti Korea Selatan dan Amerika Serikat dapat memberikan wawasan yang berguna mengenai bagaimana negara-negara tersebut mengatur kejahatan deepfake dan apakah hal tersebut bisa dijadikan acuan bagi reformulasi hukum di Indonesia. Scholarly Perspectives on Comparative Law oleh Merryman dan Parker mengemukakan bahwa perbandingan hukum berguna untuk memahami perbedaan dan persamaan dalam sistem hukum berbagai negara dan dapat menghasilkan rekomendasi terbaik dalam merumuskan kebijakan hukum nasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu suatu pendekatan yang menitikberatkan pada kajian terhadap norma-norma hukum positif yang berlaku di Indonesia. Dalam konteks ini, penelitian berfokus pada pengaturan hukum mengenai kejahatan digital berupa deepfake, yang saat ini menjadi salah satu tantangan serius dalam era perkembangan teknologi digital dan kecerdasan buatan (Artificial Intelligence/AI). Melalui pendekatan yuridis normatif, penulis menelaah aturan-aturan yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP) sebagai dasar utama untuk memahami sejauh mana regulasi yang ada mampu menjawab persoalan hukum yang ditimbulkan oleh penggunaan teknologi deepfake.

Tujuan utama dari penggunaan pendekatan ini adalah untuk mengkaji relevansi, keberlakuan, dan efektivitas peraturan perundang-undangan yang ada. Hal ini penting dilakukan karena fenomena deepfake berpotensi besar menimbulkan kerugian bagi individu maupun masyarakat, baik dalam bentuk pencemaran nama baik, penyebaran hoaks, hingga manipulasi konten untuk tujuan politik maupun kriminal. Oleh karena itu, penelitian ini berusaha menilai apakah instrumen hukum yang tersedia sudah cukup memadai dalam memberikan perlindungan, atau justru masih terdapat celah hukum (legal gap) yang perlu segera diisi melalui pembaruan regulasi.

Selain menggunakan pendekatan yuridis normatif, penelitian ini juga menerapkan pendekatan

perbandingan hukum (comparative approach). Pendekatan ini dilakukan dengan cara membandingkan aturan hukum terkait deepfake di beberapa negara yang sudah lebih dahulu menghadapi fenomena tersebut, khususnya Korea Selatan dan Amerika Serikat. Korea Selatan dikenal sebagai salah satu negara dengan kemajuan teknologi tinggi yang juga menghadapi tantangan besar akibat maraknya kasus deepfake, terutama yang berkaitan dengan pornografi digital dan penyebaran konten ilegal. Sementara itu, Amerika Serikat sebagai pusat perkembangan teknologi digital dan AI juga telah menginisiasi berbagai kebijakan hukum, baik di tingkat federal maupun negara bagian, untuk merespons penyalahgunaan deepfake.

Melalui studi perbandingan ini, penelitian berusaha menggali persamaan dan perbedaan dalam pengaturan hukum di kedua negara tersebut, serta menilai sejauh mana langkah-langkah hukum yang mereka tempuh dapat menjadi acuan atau inspirasi bagi Indonesia. Dengan demikian, hasil analisis diharapkan mampu memberikan gambaran yang lebih komprehensif mengenai opsi-opsi pembaruan hukum yang sesuai dengan kondisi sosial, politik, dan budaya hukum di Indonesia.Dengan menggabungkan pendekatan yuridis normatif dan perbandingan hukum, penelitian ini diharapkan tidak hanya menghasilkan kajian teoretis mengenai regulasi deepfake di Indonesia, tetapi juga memberikan rekomendasi praktis untuk perumusan kebijakan hukum

Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas:

1. Bahan Hukum Primer:
   a. Undang-Undang yang berlaku di Indonesia, seperti UU No. 19 Tahun 2016 tentang ITE, KUHP, dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.
   b. Peraturan Negara Lain yang mengatur tentang deepfake, khususnya dari Korea Selatan dan Amerika Serikat, sebagai bahan perbandingan.
   c. Ketentuan Hukum Internasional terkait teknologi AI dan kejahatan digital.
2. Bahan Hukum Sekunder:
   a. Buku-buku, jurnal, artikel ilmiah, dan tulisan akademik lainnya yang relevan dengan topik penelitian ini, untuk memperkaya perspektif dalam membahas regulasi tentang deepfake.
3. Bahan Hukum Tersier:
   a. Kamus Hukum dan referensi lain yang membantu dalam pemahaman istilah dan konsep hukum yang digunakan dalam penelitian ini.

Metode Pengumpulan Data

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yang mencakup penelaahan terhadap literatur hukum yang relevan, peraturan perundang-undangan, serta karya-karya ilmiah yang membahas topik deepfake dan regulasi AI di berbagai negara. Proses ini bertujuan untuk memperoleh pemahaman yang lebih dalam terkait dengan ketentuan hukum yang berlaku dan perbandingan penerapannya di negara-negara lain.

Metode Analisis

Data yang diperoleh dari studi kepustakaan akan dianalisis secara kualitatif dengan menggunakan metode deskriptif-analitis. Penulis akan menggambarkan dan menganalisis fenomena hukum terkait deepfake, baik di Indonesia maupun di negara lain, untuk memahami tantangan hukum yang dihadapi. Pola berpikir deduktif akan digunakan untuk menarik kesimpulan dari norma umum yang tercantum dalam peraturan perundang-undangan yang berlaku, serta untuk mengaitkan teori-teori hukum dengan peristiwa konkret yang terjadi, baik yang berkaitan dengan kasus deepfake maupun regulasi yang ada.

HASIL DAN PEMBAHASAN

Pengaturan Sanksi Pidana Deepfake Dalam KUHP Baru Dan UU ITE

Perkembangan teknologi digital telah membawa berbagai kemudahan dalam kehidupan manusia, namun di sisi lain juga memunculkan tantangan hukum yang kompleks. Salah satu fenomena yang terjadi sorotan global adalah kemunculan teknologi ”*deefake*”, yaitu teknologi berbasis kecerdasan buatan (*artificial intelligence*) yang memungkinkan seseorang untuk memanipulasi gambar, suara, atau video sehingga tampak menyerupai orang lain secara meyakinkan. Teknologi ini pada awalnya dikembangkan untuk tujuan hiburan dan kreativitas, namun dalam perkembangannya disalahgunakan untuk menyebarkan konten pornografi, diinformasi polotik, pencemaran nama baik, hingga penipuan daring.

Fenomena *deepfake* ini telah menimbulkan keresahan di tengah masyarakat karena mampu menciptakan realitas palsu yang sulit dibedakan dari kenyataan. Dalam Konteks hukum pidana, hal ini menjadi persoalan serius karena belum adanya ketentuan yang secara eksplisit mengatur mengenai penggunaan teknologi *deepfake* dalam sistem hukum Indonesia. KUHP Baru dan UU ITE sebagai perangkat hukum positif yang berlaku saat ini belum memiliki norma yang secara khusus mejerat kejahatan berbasis *deepfake*, sehingga memimbulkan kekosongan hukum dan ketidakpastian dalam penegakan hukum.

Negara-negara lain seperti Korean Selatan dan Amerika Serikat telah lebih dahulu merespons kejahatan ini dengan menerbitkan regulasi khusus yang mengatur penggunaan *deepfake*, terutama dalam konteks politik dan pornografi. Oleh karena itu, kajian ini penting dilakukan untuk memahami bagaimana pengaturan sanksi pidana terhadap kejahatan *deepfake* dalam kerangka hukum Indonesia saat ini, serta bagaimana perbandingannya dengan negara lain sebagai bahan evaluasi dan rekomendasi reformasi hukum pidana nasional.

KUHP Baru

Kitab Undang-Undang Hukum Pidana (KUHP) sebagai hukum pidana positif di Indonesia saat ini belum memiliki ketentuan eksplisit mengenai kejahatan berbasis kecerdasan buatan seperti *deepfake*. Namun, dalam praktiknya, penegak hukum dapat melakukan pendekatan yuridis dengan menggunakan beberapa pasal pidana konvensional untuk menjerat pelaku *deepfake.*Salah satu pasal yang sering dijadikan rujukan adalah Pasal 378 KUHP tentang penipuan. Pasal ini berbunyi. “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan suatu barang, atau supaya memberi utang maupun menghapuskan piutang, dihukum karena penipuan, dengan pidana penjara paling lama empat tahun.”

Tindak *deepfake* yang menghasilkan video manipulatif guna menipu orang lain, menyebarkan informasi palsu, atau merugikan korban secara ekonomi dapat ditafsirkan masuk dalam ranah penipuan. Namun, penggunaan pasal ini memerlukan pembuktian unsur dolus (niat jahat) serta kaitan langsung antara konten palsu dan kerugian yang dialami korban.Selain itu, Pasal 310 dan 311 KUHP tentang pencemaran nama baik juga bisa digunakan jika konten *deepfake* menyebabkan kehormatan atau nama baik seseorang tercemar. Terlebih bila video tersebut bersifat pornografis atau memuat penghinaan secara visual. Kemudian, Pasal 281 KUHP mengenai perbuatan melanggar kesusilaan dapat digunakan jika konten *deepfake* memperlihatkan tubuh atau adegan seksual yang tidak pantas. Akan tetapi, pendekatan melalui KUHP ini masih menimbulkan persoalan yuridis, sebab ketentuan-ketentuan tersebut tidak dibuat dengan mempertimbangkan kejahatan digital berbasis AI. Hal ini menunjukan adanya kekosongan hukum (legal vacuum) dan ketidaksesuaian antara jenis kejahatan modern dan instrument hukum pidana yang konvesional.

UU ITE

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) juga belum secara spesifik menyebut istilah “*deepfake*”. Namun, sejumlah pasal dalam UU ini dapat digunakan untuk menjerat pelaku penyebar konten manipulatif berbasis kecerdasan buatan

Pertama, Pasal 27 ayat (1) UU ITE menyatakan: ”Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektromik yang memiliki muatan yang melanggar kesusilaan”.

Dalam kontek ini, video *deepfake* pornografi yang menyertakan wajah seseorang tanpa persetujuan dapat dianggap sebagai pelanggaran terhadap norma kesusilaan.

Kedua, Pasal 28 ayat (1) UU ITE berbunyi:“Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.”

Pasal ini dapat digunakan bila konten *deepfake* diproduki untuk menyesatkan public atau menyebarkan hoaks dengan maksud merugikan secara ekonomi.

Ketiga, Pasal 35 UU ITE: “Setiap orang dengan sengaja dan tanpa haka tau melawan hukum melakukan menipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan informasi Elektronik dan/atau Dokumen Elektronik dengan Tujuan agar informasi tersebut dianggap seolah-olah data yang autentik.”

Pasal ini merupakan pasal yang paling relevan untuk menjerat pelaku *deepfake* karena menyangkut rekayasa visual dan audio secara digital. Namun, penerapannya bergantung pada sejauh mana penyidik dapat membuktikan adanya niat, tindakan teknis manipulasi, dan dampak terhadap korban. Secara keseluruhan, baik KUHP dan UU ITE masih belum secara eksplisit dan komprehensif

mengatur kejahatan *deepfake*. Ini menyebabkan adanya celah hukum dan perlunya pembaruan Undang-undang agar dapat mengantisipasi ancaman siber berbasis kecerdasan buatan.

Komparasi Pengaturan Deepfake di Korea Selatan dan Amerika Serikat

Perbandingan Pengaturan *Deepfake* di Korea Selatan

Pengaturan hukum terhadap teknologi deepfake di berbagai negara menunjukkan pendekatan yang berbeda-beda sesuai dengan kebutuhan dan tantangan hukum masing-masing. Korea Selatan menjadi contoh negara yang telah merespons fenomena ini dengan kebijakan dan instrumen hukum yang lebih adaptif dibandingkan Indonesia. Studi terhadap kebijakan hukum Korea Selatan penting untuk mengetahui bagaimana negara tersebut merumuskan norma hukum guna menangani kejahatan berbasis *deepfake*, sehingga dapat menjadi rujukan dalam penyusunan kebijakan hukum pidana di Indonesia.Korea Selatan merupakan salah satu negara yang secara progresif merespons ancaman teknologi deepfake, khususnya menjelang pemilihan umum. Berdasarkan revisi tahun 2023 terhadap Public Official Election Act, khususnya dalam Pasal 82-8, disebutkan: *"It is prohibited to produce, distribute, or post images or videos in which people's faces or voices are synthesized or altered using artificial intelligence technology in a way that can deceive voters, during the 90-day period before election day."*

Pelaku yang melanggar ketentuan ini dapat dijatuhi pidana penjara maksimal 7 tahun atau denda hingga 50 juta won. Pasal ini secara tegas membidik penggunaan *deepfake* untuk disinformasi politik dalam masa kampanye. Regulasi ini mencerminkn keseriusan Korea Selatan dalam menjaga integritas proses demokrasi dari ancaman manipulasi digital berbasis kecerdasan buatan. Langkah ini menjadi dapat menjadi contoh konkret bagi Indonesia dalam merumuskan kebijakan hukum yang adaptif dan relevan dengan perkembangan teknologi informasi.

Perbandingan Pengaturan Deepfake di Amerika Serikat

Amerika Serikat telah memberlakukan beberapa peraturan terkait penggunaan teknologi *deepfake*, yang umumnya ditetapkan pada tingkat negara bagian. Meskipun belum terdapat regulasi federal yang secara khusus mengatur *deepfake*, beberapa negara bagian telah mengambil langkah progresif untuk mengatasi penyalahgunaan teknologi ini, khususnya dalam konteks pemilu dan konten pornografi non-konsensual. Di California, telah diberlakukan Assembly Bill No. 602 (AB-602) pada tahun 2021. Isi pasalnya menyatakan: *"It is unlawful to distribute sexually explicit materials that depict a person engaging in sexual conduct that appears to be but is not actually that person, without their consent and with the intent to cause harm."*

UU ini mengatur deepfake pornografi sebagai pelanggaran hukum dan memungkinkan korban untuk menuntut pelaku secara perdata atau pidana. Selain itu negara bagian Texas melalui Senate Bill 751 (SB 751) melarang penggunaan deepfake untuk mempengaruhi pemilu, dengan ancaman pidana. Regulasi ini termuat dalam Texas Election Code Pasal 255.004, yang berbunyi:

"(a) A person commits an offense if, with intent ti injure a candidate or influence the result of an elestion, the person creates or causes to be created a deep fake video and causes it ti be published or distributed within 30 days of an election. (b) An offence under this section is a class A misdemeanor. (c) In this section,'deep fake video' means a video created with the intent to deceive, that appears to depict a real person perfoming an action that did not occur in reality."

("Seseorang melakukan pelanggaran apabila, dengan maksud mencemarkan nama baik seorang kandidat atau memengaruhi hasil pemilu, orang tersebut membuat atau menyebabkan dibuatnya video *deepfake* dan menyebarkannya dalam waktu 30 hari sebelum hari pemungutan suara. Pelanggaran ini tergolong sebagai pelanggaran ringan tingkat A. Dalam pasal ini, 'video *deepfake*' didefinisikan sebagai video yang dibuat dengan maksud menipu, yang tampak menggambarkan seseorang sedang melakukan tindakan yang sebenarnya tidak terjadi.") hal ini menegaskan bahwa meskipun tidak ada hukum federal yang seragam, beberapa negara bagian di AS telah merespons fenomena *deepfake* dengan regulasi yang tegas dan progresif

Ketentuan ini menunjukan bahwa negara bagian Texas telah mengambil langkah konkret dalam mengatipasi potensi ancaman *deepfake* terhadap integritas pemilu. Dengan ancaman pidan yang jelas dan cakupan yang tegas, regulasi ini dapat menjadi rujukan penting bagi negara lain, termasuk Indonesia, dalam merumuskan instrumen hukum serupa. Hal ini juga menegaskan bahwa meskipun belum terdapat hukum federal yang seragam di Amerika Serikat, beberapa negara bagian telah secara aktif merespons fenomena *deepfake* dengan pendekatan hukum yang progresif dan adaptif terhadap perkembangan teknologi

Kasus Deepfake Presiden Prabowo dalam Putusan No.124/Pid.Sus/2025/PN Gns

Dalam beberapa poin utama yang disampaikan oleh Jaksa Penuntut Umum dalam surat dakwaannya kepada Pengadilan Negeri Gunung Sugih, Lampung Tengah, terhadap terdakwa Almandela (AMA), permintaan kepada majelis hakim adalah sebagai berikut :

a. Menyatakan bahwa Terdakwa telah dengan sengaja dan tanpa hak membuat dan menyebarluaskan informasi elektronik berupa video manipulatif berbasis *deepfake* yang menampilkan tokoh-tokoh negara seperti Presiden Prabowo Subianto, Wakil Presiden, dan pejabat kementerian.
b. Menyatakan bahwa tindakan Terdakwa memenuhi unsur Pasal 35 juncto Pasal 51 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE.
c. Menyatakan bahwa Terdakwa juga telah melakukan penipuan sebagaimana diatur dalam Pasal 378 KUHP.
d. Memohon kepada Majelis Hakim untuk menjatuhkan pidana penjara kepada Terdakwa selama 5 tahun dan denda pidana sesuai ketentuan UU ITE.

Kronologi peristiwa berdasarkan hasil penyidikan Bareskrim Polri adalah sebagai berikut:

a. Pada tanggal 16 Januari 2025, Terdakwa AMA ditangkap di Lampung Tengah setelah terbukti menyebarkan video *deepfake* yang menggunakan wajah Presiden Prabowo dan sejumlah pejabat negara.
b. Hasil analisis digital dari Puslabfor Bareskrim menyatakan bahwa video tersebut merupakan hasil manipulasi deepfake dengan tingkat kemiripan 99–100%.
c. Terdakwa JS (rekan AMA) kemudian ditangkap sebagai pengembang dan penyebar jaringan konten tersebut melalui media sosial dan grup percakapan daring
d. Tindak pidana ini diproses oleh Kejaksaan Negere Lampung Tengah dan di daftarkan dalam register perkara dengan Nomor: 124/Pid.Sus/2025/PN Gns

Putusan Majelis Hakim dalam perkara ini menyatakan:

a. Menyatakan Terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana penyebaran informasi elektronik palsu dengan maksud menipu, sebagaimana dimaksud dalam dewaan primer;
b. Menjatuhkan pidana kepada Terdakwa berupa pidana penjara selama 3 tahum 6 bulan dan denda sebesar Rp 50 juta subsidair 4 bulan kurungan;
c. Menyatakan barang bukti berupa perangkat lunak dan peranglat keras yang digunakan untuk produksi video deepfake dirampas untuk dimusnakan;
d. Menghukum terdakwa untuk membayar perkara sejumlah Rp 5.000

Kasus Deepfake Pornografi Oleh ABH (Jombang), ditangani Polres Kendal- 2025

Dalam beberapa poin utama yang disampaikan oleh kepolisian resor kendal dalam siaran pers resmi, kasus ini bermula dari laporan Masyarakat yang mencurigai adanya aktivitas penyebaran konten pornografi hasil manipulasi digital berbasis kecerdasan buatan (*deepfake*) melalui platform Telegram. Setalah dilakukan patroli siber, penyidik mendeteksi akun berinisial ABH (laki-laku, 46 tahun, asal Jombang, Jawa Timur) sebagai pelaku.

a. Penyidik menyatakan bahwa pelaku menggunakan foto wajah orang lain yang dikirim oleh pemesan, kemudian menggabungkannya dengan video porno dari internet menggunakan teknologi *deepfake*
b. ABH menawarkan jasa melalui forum daring dan aplikasi Telegram untuk membuat konten dengan ”request wajah” yang akan dipasang pada video pornografi.
c. Pengiriman hasil dilakukan melalui transfer file digital setelah pembayaran dilakukan oleh pemesan

Dalam proses penangkapan, pihak kepolisian menyita sejumlah barang bukti seperti :

a. 1 unit CPU,
b. 1 monitor,
c. 1 ponsel,
d. dan beberapa alat penyimpanan data digital.

Dalam siaran tersebut, penyidik menetapkan bahwa tindakan ABH melanggar beberapa ketentuan hukum yang berlaku di Indonesia. Pelaku dijerat dengan:

a. Pasal 30 jo. Pasal 4 ayat (1) dan (2) UU No. 44 Tahun 2008 tentang Pornografi;
b. Pasal 35 jo. Pasal 9 UU Pornografi;
c. Pasal 45 ayat (1) jo. Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan UU No. 1 Tahun 2024

Namun hingga saat ini, belum ditemukan informasi resmi terkait nomor perkara dan pengadilan mana yang akan memproses kasus ini, karena kasus masih berada dalam tahap penyidikan oleh Polres Kendal. Meskipun demikian, kasus ini telah mendapatkan sorotan nasional dan menjadi preseden penting untuk mendesak adanya pengaturan eksplisit terhadap kejahatan *deepfake* dalam sistem hukum Indonesia.

KESIMPULAN DAN SARAN

Kesimpulan

Selain itu, negara-negara seperti Korea Selatan dan Amerika Serikat telah menunjukkan pendekatan hukum yang lebih progresif dalam merespons fenomena deepfake. Korea Selatan melalui Public *Official Election Act Pasal 82-8* telah melarang penyebaran konten *deepfake* dalam masa kampanye, dengan ancaman pidana hingga 7 tahun. Di Amerika Serikat, negara bagian seperti California dan Texas telah memiliki undang-undang yang mengatur larangan penyebaran konten *deepfake* dalam konteks pornografi dan pemilu, seperti yang tertuang dalam *Assembly Bill No. 602* dan *Senate Bill 751*. Regulasi-regulasi ini dapat dijadikan sebagai acuan dalam pembentukan peraturan nasional di Indonesia.

Saran

Saran dari penulis yang bisa di upaya kan oleh pemerintah Indonesia melalui pembuat undang-undang perlu melakukan revisi terhadap KUHP dan UU ITE atau menyusun undang-undang baru yang secara khusus mengatur kejahatan berbasis teknologi kecerdasan buatan, termasuk deepfake. Perumusan norma baru harus mencakup definisi, jenis perbuatan yang dilarang, serta sanksi pidana yang sesuai dengan tingkat ancaman yang ditimbulkan.Pengaturan hukum tersebut harus dirancang tidak hanya untuk merespons dampak negatif deepfake dalam ranah moral atau ekonomi, tetapi juga dalam konteks ancaman terhadap demokrasi dan keamanan digital.

Oleh karena itu, studi komparatif terhadap sistem hukum di negara lain seperti Korea Selatan dan Amerika Serikat sangat penting untuk dijadikan rujukan dalam pembentukan kebijakan hukum yang adaptif dan futuristik. Penegak hukum juga perlu diberikan pelatihan dan peningkatan kapasitas dalam mendeteksi dan membuktikan tindak pidana yang melibatkan teknologi deepfake, mengingat kompleksitas teknis dan dampak sosial yang ditimbulkannya. Dengan adanya pembaruan hukum yang komprehensif, diharapkan Indonesia mampu menghadapi tantangan hukum di era digital dan memberikan perlindungan yang maksimal terhadap masyarakat dari ancaman kejahatan berbasis teknologi kecerdasan buatan

DAFTAR PUSTAKA

Amanda, S., Sijabat, U., & Lukitasari, D. (2024). Konten Gambar dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik. 13(2), 179–194. https://doi.org/10.20961/recidive.v13i2.86771

Budhijanto Danrivanto. (2023). HUKUM PERLINDUNGAN DATA PRIBADI DI INDONESIA : Cyberlaw & Cybersecurity (1st ed.). Pt. Refika Aditama.

Budhijanto Danrivanto. (2025). HUKUM CYBERCRIME 4.0 : Kejahatan Digital dan Artificial Intelligence (AI)) (1st ed.). Pt. Refika Aditama.

Chatterjee, M. (2025, May 19). Trump signs Take It Down Act, criminalizing deepfake and revenge porn. Https://Www.Politico.Com/News/2025/05/19/Trump-Signs-Take-It-down-Act-Criminalizing-Deepfake-and-Revenge-Porn-00357151?Utm.

Fauzyah, R. N., Hafidati, P., & Sunarya, S. (2024). PERLINDUNGAN HUKUM TERHADAP KORBAN TINDAK PIDANA PEMBUAT VIDEO PORNOGRAFI PALSU (DEEPFAKE PORN) BERBASIS ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA. In Lex Veritatis (Vol. 3, Issue 3). https://doi.org/10.33592/jlv.v3i3

Hyunsu, Y. (2024, September 26). South Korea to criminalise watching or possessing sexually explicit deepfakes. Https://Www.Reuters.Com/World/Asia-Pacific/South-Korea-Criminalise-Watching-or-Possessing-Sexually-Explicit-Deepfakes-2024-09-26/?

Jonaedi Efendi. (2018). Metode Penelitian Hukum: Normatif dan Empiris (1st ed.). Prenada Media.

Latifatunnisa, R., & Yudha Wira, M. (2025). URGENSI PEMBARUAN REGULASI DALAM MENANGGULANGI PENYALAHGUNAAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DAN DEEPFAKE DI INDONESIA: PERSPEKTIF PERLINDUNGAN HAK PRIVASI. Jurnal Hukum dan Kewarganegaraan, 11. https://doi.org/10.3783/causa.v11i1.11617

Lu, S. (2025, May 9). Take It Down Act: Tackling Nonconsensual Deepfakes. Https://Www.Miragenews.Com/Take-It-down-Act-Tackling-Nonconsensual-1457081/?Utm.

Putra Wicaksana, B. K., & Dewi Prima Arya, A. G. (2024). URGENSI PENGATURAN TINDAK PIDANA DEEPFAKE PORNOGRAFI DI INDONESIA. J-KIs: Jurnal Komunikasi Islam, 13(1), 530–541. https://doi.org/10.24843/KW.2024.v13.i10.p5

Schuldt, L. (2024, October 9). Every Fake You Make. Https://Verfassungsblog.de/Fake-News-Content-Moderation-Singapoer-South-Korea-Election/. https://doi.org/10.59704/d01a5685d920b50f

Shevila Kristiyenda, Y., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang. Jurnal Politik, Sosial, Hukum dan Humaniora Volume 3 Nomor 2 April 2025, 3, 149–164. https://doi.org/10.59246/aladalah.v2i4