UIRLawReview
Volume (9) Issue (1) , 2025
P-ISSN: 2548-7671, E-ISSN: 2548-768X

The Role of Law in Addressing the Spread of Deepfake Content for Digital Identity Fraud

Peran Hukum dalam Menangani Penyebaran Konten Deepfake untuk Penipuan Identitas Digital

Hazmin Sulton Firdaus[1], Lona Puspita[2]

[1]Fakultas Hukum, Universitas Terbuka, *e-mail:* hazminsf@gmail.com
[2]Fakultas Hukum, UniversitasTamansiswa Padang : lovelylona6969@gmail.com

Abstract: *Currently, the development of artificial intelligence technology has given rise to the phenomenon of Deepfake, a technology capable of realistically manipulating images, sounds, and videos, making them difficult to distinguish from the original content. Although the development of artificial intelligence technology has the potential for positive uses, such as in the world of entertainment and education, Deepfake can also pose significant risks in the current technological era, especially in terms of digital identity fraud. With the development of artificial intelligence technology, a new, serious problem has arisen, one of which is the misuse of Deepfake, which is part of artificial intelligence. The purpose of this research is to determine the role of law in overcoming the spread of deepfake content for digital identity fraud. The method used in this research is a normative legal research method with the main data source being secondary legal materials consisting of laws and regulations as well as reference books and journals. The research results state that current regulations are not able to protect victims or prevent the spread of deepfake content effectively. Therefore, improvements to existing regulations are needed to provide protection and legal certainty for deepfake victims. In addition, cross-sector collaboration is needed to overcome the challenges posed by deepfake technology.*

Keywords: *Deepfake; Law; Digital identity fraud; Regulation; Technology;*

Abstrak: Saat ini, dalam proses perkembangan teknologi kecerdasan buatan, telah memunculkan sebuah fenomena *Deepfake*, yaitu teknologi yang mampu dalam melakukan manipulasi citra, suara, dan video secara realistis sehingga akan sulit dibedakan dari konten aslinya. Meskipun dalam perkembangan teknologi kecerdasan buatan yang memiliki potensi untuk penggunaan pada hal yang positif, seperti dalam dunia hiburan dan pendidikan, *Deepfake* juga dapat menimbulkan risiko besar pada era teknologi saat ini, terutama dalam hal penipuan identitas digital. Dengan adanya perkembangan teknologi kecerdasan buatan ini maka timbul suatu permasalahan baru yang serius, salah satunya adalah dalam penyalahgunaan *Deepfake* yang menjadi bagian dari *artificial intelligence*. Tujuan penelitian yakni untuk mengetahui bagaimana peran hukum dalam pengatasi penyebaran konten *deepfake* untuk penipuan identitas digital. Metode yang digunakan dalam penelitian ini yakni metode penelitian hukum normatif dengan sumber data utama yakni bahan hukum sekunder yang terdiri dari peraturan perundang-undangan serta buku referensi dan jurnal. Hasil Penelitian menyatakan bahwa regularasi yang ada saat ini belum dapat melindungi korban atau mencegah penyebaran konten *deepfake* secara efektif. Oleh karena itu diperlukan perbaikan dari regulasi yang ada saat ini sehingga dapat memberikan perlindungan dan kepastian hukum bagi korban *deepfake.* Selain itu dibutuhkan juga kolaborasi lintas sektor guna mengatasi tantangan yang ditimbulkan oleh teknologi *deepfake*.

Kata Kunci: *Deepfake*; Hukum; Penipuan identitas digital; Regulasi; Teknologi;.

1. Pendahuluan

Kemajuan yang sangat pesat dalam bidang kecerdasan buatan (*Artificial Intelligence/*AI) saat ini telah berhasil menghadirkan suatu teknologi digital yang semakin canggih dan sulit untuk dibedakan dari konten-konten asli (Raharjo, 2023). Teknologi digital ini kemudian dikenal dengan istilah *Deepfake.* Perkembangan teknologi AI yang kian maju ini telah memicu munculnya ancaman- ancaman baru yang sangat serius bagi keamanan digital secara global, khususnya dalam konteks permasalahan penipuan identitas digital. Keberadaan *Deepfake* yang semakin sulit untuk dideteksi dan dibedakan dari konten asli telah menjadi salah satu tantangan utama yang harus dihadapi dalam upaya menjaga keamanan serta integritas identitas digital di tengah era teknologi yang terus berkembang pesat saat ini. Penyalahgunaan teknologi *Deepfake* ini telah menimbulkan berbagai macam tantangan hukum dan etika yang cukup serius, sehingga memunculkan banyak pertanyaan mengenai batasan-batasan hukum yang harus diterapkan dalam menangani kasus-kasus penipuan identitas digital yang disebabkan oleh kehadiran teknologi *Deepfake*.

Kejahatan digital atau kejahatan siber merupakan bentuk kejahatan yang keberadaannya justru tercipta akibat pesatnya perkembangan teknologi AI saat ini. Kejahatan- kejahatan tersebut seringkali dipicu atau bahkan didorong oleh kemajuan teknologi yang semakin canggih dari waktu ke waktu. Penyalahgunaan *Artificial Intelligence* dalam berbagai aktivitas kejahatan digital ini tentu membawa dampak negatif yang signifikan dan sangat merugikan bagi kehidupan masyarakat secara luas. Teknologi *Deepfake* pada umumnya berkaitan langsung dengan kemampuan modifikasi atau manipulasi berbagai bentuk konten digital seperti gambar, video, bahkan suara dengan memanfaatkan kecerdasan buatan (Santoso, 2023). Penyalahgunaan *Artificial Intelligence* dalam berbagai macam bentuk ini jelas merupakan ancaman yang harus dihadapi oleh masyarakat. Hal tersebut menjadi tantangan tersendiri bagi pemerintah dan para pemangku kepentingan lainnya untuk dapat melawan dan mengatasi teknik-teknik kejahatan digital yang semakin canggih serta sulit untuk diatasi pada saat ini.

Dengan adanya perkembangan teknologi informasi komunikasi membawa dampak positif dan negatif. Keberadaan teknologi *Deepfake* dapat menyebabkan kerugian bagi banyak orang serta dapat menimbulkan suatu tindak pidana contohnya yaitu penipuan, pornografi dan lainnya. Tindak pidana memang sudah diatur dalam KUHP akan tetapi dampak yang ditimbulkan oleh adanya teknologi *Deepfake* yang disalahgunakan akan berdampak lebih besar dibandingkan dengan tindak pidana penipuan biasanya. Saat ini, bentuk dari perlindungan korban tindak pidana atas penyalahgunaan teknologi *Deepfake* masih diragukan, karena belum adanya regulasi yang mengatur tentang adanya tindak pidana *Deepfake* tersebut. Indonesia yang merupakan negara hukum yang sudah semestinya mempunyai regulasi dalam mengatur penggunaan *Artificial Intelligence* khususnya pada tindak pidana *Deepfake*. Para penegak hukum akan kesulitan dalam mengatasi tindak pidana *Deepfake* karena belum adanya regulasi yang mengatur hal tersebut dan karena tidak adanya regulasi tersebut maka terjadilah kekosongan hukum yang dimana tidak seorangpun dapat dijatuhi pidana tanpa ada aturan yang mengaturnya (Mufi, et.al, 2024).

Pembentukan regulasi terkait dengan adanya perkembangan *Artificial Intelligence* saat ini sangat penting karena dampak negatif dari penyalahgunaan AI sangatlah nyata dan dengan adanya pembentukan regulasi terkait AI maka dalam penggunaan AI dapat dibatasi agar tidak disalahgunakan untuk suatu hal yang negatif seperti penipuan identitas digital. Dan dengan adanya regulasi tersebut maka akan memberikan manfaat yang maksimal bagi masyarakat tanpa perlu mengorbankan hak masyarakat seperti privasi dan keamanan individu.

Di Indonesia, penyalahgunaan teknologi *Deepfake* menimbulkan tantangan besar dalam aspek hukum. Meskipun Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) telah diterapkan, akan tetapi peraturan ini masih memiliki keterbatasan dalam menangani kejahatan berbasis AI yang semakin komplek. Oleh sebab itu, pada penelitian ini memiliki tujuan untuk mengeksplorasi peran hukum dalam mengatasi penyebaran konten *Deepfake* guna penipuan identitas digital dan memberikan rekomendasi untuk perbaikan regulasi di Indonesia.

Penelitian ini bertujuan untuk mengkaji berbagai tantangan yang dihadapi dalam penegakan hukum terkait penyalahgunaan teknologi *Deepfake* di Indonesia, termasuk kesenjangan regulasi dan keterbatasan teknis dalam mendeteksi serta mengatasi konten manipulatif. Dan mengevaluasi efektivitas peraturan perundang-undangan yang ada, seperti UU ITE dan UU PDP, dalam memberikan perlindungan terhadap korban kejahatan *Deepfake*.

2. Metode

Pada penelitian ini menggunakan pendekatan yuridis normatif dengan menggunakan metode studi literatur. Data yang digunakan pada penelitian ini menggunakan data sekunder yang berasal dari Undang-Undang, jurnal akademik, artikel hukum yang relevan dengan topik *Deepfake* dan penipuan identitas digital. Analisis pada penelitian ini dilakukan secara deskriptif kualitatif untuk menggambarkan peran dan efektivitas hukum dalam menghadapi penyalahgunaan *Deepfake*.

3. Pembahasan

A. Perkembangan *Deepfake* di Indonesia

Perkembangan teknologi pada bidang kecerdasan buatan (*Artificial Intelligence*) menghadirkan banyak dampak yang signifikan dalam aspek kehidupan. Salah satu contohnya yaitu hadirnya teknologi *Deepfake* yang dimana *Deepfake* merupakan suatu teknologi yang menggunakan teknologi kecerdasan buatan atau *Artificial Intelligence* (AI) guna untuk menciptakan suatu video maupun gambar palsu yang sangat meyakinkan yang dimana wajah seseorang dapat diganti dengan wajah orang lain dengan tujuan untuk melakukan penipuan identitas. Dalam sejarahnya, *Deepfake* pertama kali dimulai dari penggunaan teknologi kecerdasan buatan dan algoritma pemrosesan dalam menggabungkan wajah seseorang ke dalam foto maupun video. Dengan seiring waktu perkembangan AI terutama pada teknologi *Deepfake* menjadi sangat pesat yang dimana pada awalnya *Deepfake* hanya dapat mengubah foto maupun video, saat ini dengan

perkembangan yang pesat tersebut *Deepfake* dapat mengubah atau manipulasi suara seseorang dalam suatu video. Dampak dari perkembangan teknologi tersebut menjadi fokus utama dalam keamanan dan privasi yang dimana mengingat potensinya dari teknologi tersebut, dalam menyebarkan informasi palsu maupun merusak reputasi dari seseorang secara signifikan.

Deepfake, sebagai sebuah teknologi yang dapat memanipulasi konten audio dan visual yang berbasis pada kecerdasan buatan (*Artificial Intelligence*), semakin marak dipergunakan pada konteks yang tidak etis, termasuk pada penipuan identitas digital. Fenomena tersebut menimbulkan risiko yang serius bagi individu atau pun organisasi, karena hal tersebut dapat memungkinkan pelaku kejahatan untuk melakukan manipulasi informasi identitas seseorang secara realistis. Selain itu, ancaman lainnya adalah manipulasi kecerdasan buatan itu sendiri, yang dimana pihak tidak bertanggung jawab dapat menyisipkan data yang salah atau merancang serangan untuk menghasilkan keluaran yang tidak diinginkan (Santoso, J. T., 2023). Kini, ketika AI mampu menghasilkan konten palsu yang semakin canggih, seperti video sintetis yang dapat menggantikan wajah seseorang dengan sangat akurat (Muttaqin et al., 2023), risiko dalam penyalahgunaan menjadi lebih besar. Oleh karena itu, diperlukannya regulasi yang tidak hanya mengatur penggunaan teknologi ini tetapi juga dapat melindungi korban yang terdampak. Perlindungan data pribadi adalah isu yang semakin penting dan mendesak untuk ditangani di tengah meningkatnya ancaman *cybercrime* (Yamin, et al, 2022).

Teknologi *Deepfake* terus berkembang dengan cepat seiring kemajuan dalam algoritma *deep learning*. Teknologi ini memungkinkan pembuatan konten manipulatif yang sangat realistis, termasuk video dan audio, yang sangat dengan mudah menyebarkan melalui media sosial dan platform digital lainnya. Dampak dari penyebaran konten *Deepfake* sangat luas dan berpotensi merusak, mencakup penipuan identitas, pencemaran nama baik, dan manipulasi opini publik. Teknologi *Deepfake* memungkinkan penggantian wajah seseorang dalam video sehingga tampak seperti orang lain (Respati et al, 2024)

Deepfake juga digunakan untuk menyebarkan informasi yang menyesatkan dalam berbagai konteks, seperti politik, bisnis, dan sosial. Hal tersebut menimbulkan tantangan serius bagi otoritas hukum dalam menjaga kebenaran informasi dan kepercayaan publik. Konten *Deepfake* yang digunakan dalam menjaga kebenaran informasi atau tindakan seseorang dapat memicu konsekuensi serius, termasuk kerugian finansial dan reputasi korban. Dengan perkembangan teknologi informasi yang sangat pesat, masyarakat menghadapi perubahan besar, baik positif maupun negatif yang berdampak pada budaya dan peradaban manusia itu sendiri (Agung et al., 2023).

Selain dampak hukum, privasi data pribadi juga menjadi perhatian besar. Teknologi *Deepfake* sering kali bergantung pada data biometrik, seperti wajah atau suara, yang

diakses tanpa izin pemiliknya. Kecerdasan buatan mendapatkan data pribadi secara mudah melalui akses ke Maha Data yang mengumpulkan berbagai data dari para pengguna. Data ini kemudian dimanfaatkan untuk menciptakan konten manipulatif tanpa se pengetahuan individu yang bersangkutan, dan dapat menimbulkan risiko privasi yang serius (Andika & Soemarno, 2023). *Deepfake* juga tidak hanya berdampak pada aspek hukum dan privasi tetapi juga menimbulkan tantangan etika. Etika adalah prinsip moral yang mengatur tingkah laku seseorang atau pelaksanaan suatu kegiatan (Budi Raharjo,2020). Dalam konteks ini, pengembangan dan penggunaan *Deepfake* harus didasarkan pada prinsip-prinsip etika untuk mencegah penyalahgunaan yang merugikan. Akan tetapi, Penggunaan AI tanpa pengawasan sangat berbahaya, karena meskipun AI memiliki kecerdasan, program ini tidak memiliki moral (Mufti et al, 2024).

Dampak sosial lain dari teknologi ini ialah *Cyberstalking*, di mana pelaku menggunakan teknologi untuk mengganggu atau merendahkan korban. *Cyberstalking* memungkinkan pelaku mengakses data pribadi korban dan menyalahgunakan nya untuk kepentingan pribadi mereka sendiri (Yusuf et al, 2024). Hal ini menunjukkan bahwa teknologi *Deepfake* sering kali digunakan untuk tujuan jahat yang secara langsung merugikan individu tertentu. Manipulasi ini menunjukkan bahwa ancaman dari *Deepfake* tidak hanya terletak pada hasil akhirnya akan tetapi juga pada proses penciptaan nya. *Deepfake* juga dapat menciptakan bentuk pelecehan baru yang sebelumnya tidak terbayangkan. Pengembangan perangkat lunak yang dapat menggantikan wajah seseorang dalam video secara akurat memperbesar risiko pelecehan dan penyebaran konten palsu yang sulit dibedakan dari kenyataan (Muttaqin et al, 2023). Hal ini menunjukkan bahwa perkembangan teknologi *Deepfake* memerlukan pengawasan ketat untuk mencegah dampak negatif yang meluas. Oleh karena itu maka regulasi yang kuat dan responsif penting untuk mengatasi tantangan ini. Regulasi tersebut tidak hanya akan melindungi masyarakat dari penyalahgunaan teknologi tetapi juga memberikan landasan hukum yang jelas bagi aparat penegak hukum.

B. Pengaturan *Deepfake* di Indonesia

Indonesia telah memiliki beberapa peraturan yang mengatur kejahatan siber, namun regulasi yang secara khusus menargetkan teknologi *Deepfake* masih belum tersedia. UU ITE No. 19 Tahun 2016 menjadi landasan hukum utama dalam menangani pelanggaran di ranah digital. Pasal 27 Aya (3) UU ITE menyatakan larangan distribusi informasi yang bersifat penghinaan atau pencemaran nama baik, sementara pada Pasal 28 Ayat (1) melarang penyebaran berita bohong yang dapat menyebabkan kerugian. Dalam konteks *deepfake* pasal- pasal ini dapat diterapkan pada kasus di mana konten tersebut digunakan untuk merusak reputasi atau menipu pihak lain.

Selain itu, UU PDP memberikan kerangka hukum terkait pengelolaan data pribadi. Pada Pasal 65 UU PDP menegaskan bahwa dalam penggunaan data pribadi haruslah

digunakan dengan adanya persetujuan pemilik data. Namun, UU ini tidak secara eksplisit mencakup penggunaan data pribadi dalam pembuatan konten *Deepfake*. ketidakpastian hukum dalam memberikan perlindungan terhadap korban *Deepfake* (Noerman & Ibrahim, 2024). Akan tetapi, dalam penerapan pasal-pasal tersebut sering kali menemui kendala, terutama karena sifat teknologi *Deepfake* yang canggih dan sulit dibedakan antara konten asli dan konten hasil dari manipulasi *Deepfake*. *Deepfake* sendiri mempunyai kemampuan dalam menciptakan rekayasa audio, visual, maupun kombinasi keduanya yang sehingga terlihat sangat nyata. Dalam kasus tertentu,seperti penyebaran video *Deepfake* seorang tokoh masyarakat yang memberikan pernyataan palsu, pembuktian tindak pidana ini memerlukan keahlian forensik digital yang tidak selalu dimiliki oleh aparat penegak hukum. Hal tersebut mengakibatkan proses penyelidikan menjadi lambat dan kurang efektif. Selain itu juga, belum adanya aturan eksplisit yang secara nyata mengatur teknologi manipulasi visual dan audio seperti *Deepfake*, juga menjadikan penegak hukum bergantung pada interpretasi pasal-pasal umum yang ada dalam UU ITE, sehingga ruang lingkup perlindungan terhadap korban menjadi terbatas.

Di sisi lain, UU PDP memberikan kerangka hukum yang lebih spesifik terkait pengelolaan data pribadi di Indonesia. Pada Pasal 65, UU PDP menegaskan bahwa penggunaan data pribadi harus dilakukan dengan persetujuan eksplisit dari pemilik data. Aturan tersebut, meskipun memberikan perlindungan terhadap data biometrik seperti wajah, suara, atau sidik jari, tetap memiliki kekurangan dalam menangani penyalahgunaan data pribadi untuk pembuatan konten *Deepfake*. Hal ini dikarenakan UU PDP tidak secara eksplisit mencantumkan mekanisme penanganan pelanggaran berbasis teknologi AI, seperti *Deepfake*, yang memanfaatkan data biometrik untuk tujuan manipulasi. *Deepfake* pornografi menggambarkan kekhawatiran terkait pemalsuan video yang memanfaatkan kecerdasan buatan untuk menciptakan konten palsu yang sangat sulit dibedakan dari yang asli (Rizki K, 2024).

Ketiadaan regulasi yang spesifik ini menimbulkan sejumlah permasalahan, Pertama, korban penyalahgunaan *Deepfake* sering kali tidak memiliki jalur hukum yang jelas untuk memperjuangkan hak mereka. Misalnya, seseorang yang menjadi korban pembuatan video *Deepfake* pornografi dengan wajahnya yang dimanipulasi akan menghadapi kesulitan dalam membuktikan kerugian secara langsung. Dalam banyak kasus, pelaku kejahatan menggunakan teknologi *Deepfake* untuk tujuan eksploitasi seksual, penipuan, atau bahkan politik, namun tetap lolos dari jerat hukum karena belum ada pasal yang secara spesifik mengatur tindak pidana tersebut. Meskipun kasus semacam itu sering terjadi dan menimbulkan kerugian signifikan bagi banyak orang, keterbatasan pengaturan hukum membuat aparat hukum kesulitan menjerat pelaku (Novera & Z, 2024).

Dalam konteks ini, *Deepfake* digunakan untuk tujuan disinformasi yang berpotensi menciptakan polarisasi di masyarakat. Meskipun konten seperti ini dapat dilaporkan sebagai suatu pelanggaran UU ITE Pasal 28 Ayat (1), proses hukum sering kali terhambat oleh kurangnya bukti teknis yang valid untuk membuktikan bahwa konten tersebut merupakan hasil dari manipulasi teknologi. Kasus penipuan identitas digital tidak hanya merugikan korban yang ditipu secara finansial akan tetapi juga merusak reputasi dari korban tersebut. Meskipun pelaku dapat dijerat dengan pasal tentang penipuan identitas, dalam proses penegakan hukum akan tetap sulit dilakukan tanpa adanya regulasi yang mencakup spesifikasi teknologi *Deepfake*. Oleh karena itu, urgensi untuk mengembangkan regulasi yang adaptif dan responsif menjadi semakin mendesak (Syaifudin, 2024).

C. Perbandingan pengaturan *deepfake* di Indonesia dengan regulasi internasional

Di tingkatan internasional, terdapat beberapa negara yang telah mengadopsi sistem regulasi yang lebih ketat dalam menangani *Deepfake*. Contoh salah satunya ialah Uni Eropa dengan *General Data Protection Regulation* (GDPR) yang menerapkan standar tinggi dalam perlindungan data pribadi, termasuk penggunaan data digital. *General Data Protection Regulation* (GDPR) menekankan prinsip "*Data protection by design*" yang berarti setiap teknologi yang digunakan untuk mengelola data pribadi harus menerapkan langkah-langkah keamanan sejak awal pengembangan nya. Praktik tersebut dapat menjadi contoh bagi Indonesia untuk memperkuat regulasi domestik terkait *Deepfake*. *General Data Protection Regulation* (GDPR) juga mewajibkan transparansi dalam penggunaan data, yang dapat diterapkan pada pengembangan teknologi AI (*Artificial Intelligence*) untuk mencegah penyalahgunaan dalam pembuatan konten manipulatif. Penguatan hukum di Indonesia perlu mencakup regulasi yang mengintegrasikan perlindungan data pribadi dengan kontrol atas penggunaan teknologi AI (*Artificial Intelligence*).

Selain Uni Eropa, negara bagian California di Amerika Serikat juga telah mengambil langkah maju dengan menerapkan regulasi seperti *California Consumer Privacy Act* (CCPA) dan Undang- Undang khusus untuk mengatur penggunaan *Deepfake*. Misalnya, undang-undang California melarang penggunaan *Deepfake* dalam konteks politik menjelang pemilu dan melarang penggunanya untuk menciptakan contoh konkret bagaimana regulasi dapat dibuat untuk mengatasi dampak sosial dan politik yang merugikan dari teknologi manipulatif seperti *Deepfake*. Perbandingan dengan negara-negara ini memberikan pelajaran penting bagi Indonesia dalam memperkuat regulasi domestik terkait *Deepfake*. Salah satu langkah yang dapat diambil adalah mengadopsi prinsip transparansi dan keamanan seperti yang diterapkan GDPR. Sebagai contoh, Indonesia dapat menerapkan kebijakan yang digunakan telah mendapat persetujuan

eksplisit dari pemiliknya. Selain itu, regulasi ini dapat mencakup kewajiban bagi platform digital untuk menyediakan alat pendeteksi *Deepfake* guna melindungi pengguna dari potensi manipulasi.

D. Implikasi *Deepfake* terhadap Identitas Digital dan Privasi

Teknologi *Deepfake* memiliki dampak yang signifikan pada identitas digital dan privasi individu. Konten *Deepfake* yang bersifat penipuan identitas digital menyerupai salah satunya dalam bentuk pornografi yang dimana hal tersebut merupakan tindakan kriminal yang dapat menimbulkan trauma psikologis yang mendalam bagi para korban. *Deepfake* pornografi merupakan ancaman besar karena sulitnya membedakan antara konten asli dan palsu. Dampak atas tindakan kriminal tersebut meluas ke reputasi individu, karier, dan hubungan sosial, serta menimbulkan kerugian material yang signifikan (Kurniarullah et al, 2024). Dalam Pasal 27 Ayat (1) UU ITE telah melarang penyebaran konten yang melanggar kesusilaan yang dimana hal tersebut termasuk pada konten pornografi. Akan tetapi, aspek visual dan manipulasi AI dalam konten *Deepfake* belum diatur secara spesifik dalam peraturan tersebut. Hal ini menunjukkan bahwa diperlukannya revisi maupun tambahan peraturan yang secara eksplisit mengatur penggunaan dan penyebaran konten *Deepfake*.

Implikasi dari ketidakpastian hukum ini tidak hanya dirasakan oleh korban individu, akan tetapi juga oleh institusi yang bertanggung jawab dalam penegakan hukum. Penegak hukum di Indonesia sering kali menghadapi tantangan teknis dalam mengidentifikasi dan mengatasi kejahatan berbasis *Deepfake*. Kurangnya pelatihan dan sumber daya untuk mengelola teknologi canggih seperti *Deepfake* menyebabkan proses investigasi menjadi terhambat. Selain itu juga, kurangnya kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat sipil juga memperburuk situasi. Sebagai contoh, platform teknologi yang digunakan untuk menyebarkan konten *Deepfake* sering kali tidak bekerja sama secara proaktif untuk menghapus konten yang melanggar atau menyediakan data teknis yang dapat membantu proses dalam penyelidikan.

Dalam kasus tertentu, penyebaran konten *Deepfake* bahkan dapat digunakan untuk tujuan pemerasan. Pelaku membuat atau menyebarkan video *Deepfake* dengan tujuan mencemarkan nama baik korban dan menuntut sejumlah uang sebagai imbalan untuk tidak menyebarkan konten tersebut lebih lanjut. Hal ini tidak hanya melukai martabat korban tetapi juga menimbulkan kerugian ekonomi yang signifikan. Korban sering kali merasa terjebak dalam situasi tanpa jalan keluar, terutama ketika tidak ada jaminan hukum yang memadai untuk melindungi mereka dari penyebaran konten lebih lanjut.

Selain dampak langsung terhadap korban individu, implikasi sosial yang lebih luas dari teknologi *Deepfake* juga perlu diperhatikan. Dalam era digital, kepercayaan publik

terhadap informasi visual dan audio mulai terkikis. Ketika teknologi seperti deepdake memungkinkan siapa saja untuk menciptakan konten digital. Hal ini berpotensi menciptakan lingkungan informasi yang penuh ketidakpastian dan ketidakpercayaan, yang pada akhirnya dapat merusak stabilitas sosial dan demokrasi.

Untuk mengatasi berbagai implikasi negatif ini, pendekatan holistik sangat diperlukan. Regulasi yang komprehensif harus segera dirancang untuk mencakup semua aspek penggunaan teknologi *Deepfake*, termasuk pencegahan penyalahgunaan, mekanisme deteksi, dan penegakan hukum. Selain itu, pelatihan teknis untuk penegak hukum harus ditingkatkan agar mereka dapat mengidentifikasi dan mengatasi kejahatan berbasis teknologi ini secara efektif. Peningkatan kesadaran di masyarakat juga merupakan langkah penting dalam menghadapi ancaman teknologi *Deepfake*. Publik perlu diberi pemahaman tentang cara mengenali konten *Deepfake* dan melaporkan penyalahgunaan nya. Selain itu, kolaborasi antara pemerintah, perusahaan teknologi, dan lembaga pendidikan dapat membantu menciptakan lingkungan digital yang lebih aman dan terpercaya.

Melalui langkah-langkah tersebut diharapkan dampak negatif dari teknologi *Deepfake* terhadap identitas digital dan privasi individu dapat diminimalkan. Regulasi yang kuat, kerja sama lintas sektor, dan pemberdayaan masyarakat merupakan kunci untuk menghadapi tantangan yang ditimbulkan oleh teknologi canggih ini di era digital.

E.Tantangan teknis dalam penegakan hukum *deepfake* di Indonesia

Penegakan hukum dalam kasus *Deepfake* dihadapkan pada berbagai tantangan teknis. Proses identifikasi dan deteksi konten *Deepfake* membutuhkan teknologi canggih, seperti forensik digital berbasis AI dan algoritma *machine learning*. Teknologi tersebut sangat penting dalam mengidentifikasi tanda-tanda manipulasi pada gambar dan audio, akan tetapi dalam pengadopsian nya di Indonesia masih terbatas. Regulasi yang adaptif dan kolaborasi lintas sektor adalah kunci untuk menghadapi tantangan teknologi baru (Syaifudin, 2024).

Sumber daya manusia yang memiliki keahlian di bidang forensik digital juga masih terbatas. Dan kurangnya pelatihan bagi aparat penegak hukum menghambat upaya deteksi dan penegakan hukum secara efektif. Oleh sebab itu, maka diperlukannya adanya investasi dalam pengembangan sumber daya manusia serta peningkatan kolaborasi dengan sektor teknologi untuk memperkuat kapabilitas deteksi dan investigasi. Tanpa infrastruktur yang memadai, baik dalam bentuk perangkat lunak maupun perangkat keras, penegakan hukum akan terus berada dalam posisi yang lemah ketika berhadapan dengan kejahatan berbasis *Deepfake*.

Salah satu hambatan utama dalam konteks ini ialah kurangnya sumber daya manusia yang memiliki keahlian di bidang forensik digital. Forensik digital merupakan

disiplin yang memerlukan pemahaman mendalam tentang teknologi informasi, keamanan siber, dan analisis data. Saat ini jumlah aparat penegak hukum di Indonesia yang memiliki keterampilan khusus di bidang ini masih sangat terbatas. Ditambah lagi, pelatihan yang diberikan kepada aparat penegak hukum sering kali belum mencakup teknologi canggih seperti *Deepfake*, yang terus mengalami evolusi dengan kecepatan tinggi.

Kurangnya pelatihan bagi aparat penegak hukum menyebabkan upaya deteksi dan investigasi terhadap konten *Deepfake* menjadi terhambat. Misalnya, dalam kasus manipulasi visual yang kompleks, diperlukan algoritma khusus untuk mendeteksi anomali dalam pola *pixel*, pencahayaan, atau sinkronisasi audio dengan gerakan bibir. Akan tetapi, jika aparat penegak hukum tidak memiliki akses atau pemahaman terhadap teknologi ini, investigasi menjadi tidak efektif. Situasi ini diperburuk oleh fakta bahwa pelaku kejahatan sering kali menggunakan teknologi yang lebih maju dibandingkan dengan alat yang tersedia di lembaga penegak hukum.

Selain masalah teknologi dan sumber daya manusia, tantangan lain terletak pada kurangnya kolaborasi antara pemerintah, sektor teknologi, dan institusi terkait lainnya. Banyak perusahaan teknologi yang memiliki kemampuan untuk mendeteksi dan menghapus konten *Deepfake* di platform mereka, tetapi sering kali tidak ada mekanisme yang memadai untuk berbagai informasi atau bekerja sama dengan pihak berwenang. Padahal, kolaborasi semacam ini sangat penting untuk mempercepat proses investigasi dan mencegah penyebaran konten *Deepfake* lebih lanjut. Sebagaimana yang disampaikan, perlindungan data pribadi adalah isu yang semakin penting dan mendesak untuk ditangani di tengah meningkatnya ancaman *cybercrime* (Yamin et al., 2022).

Untuk mengatasi tantangan ini, maka investasi dalam pengembangan sumber daya manusia menjadi suatu keharusan. Pemerintah perlu mengalokasikan dana untuk menyediakan pelatihan forensik digital yang mendalam bagi aparat penegak hukum. Pelatihan ini harus mencakup pemahaman tentang cara kerja teknologi *Deepfake*, metode deteksi, serta teknik investigasi relevan. Selain itu, lembaga pendidikan tinggi juga dapat berperan dengan menawarkan program studi atau pelatihan khusus di bidang forensik digital dan keamanan siber.

Di sisi lain, kolaborasi dengan sektor teknologi harus diperkuat. Perusahaan teknologi yang memiliki akses algoritma pendeteksian *Deepfake* dapat membantu pihak berwenang dalam mengembangkan perangkat lunak yang efektif untuk keperluan investigasi. Selain itu, pemerintah dapat menjalin kerja sama dengan komunitas teknologi global untuk berbagi pengetahuan, alat, dan sumber daya yang diperlukan dalam menangani ancaman *Deepfake*. Penguatan regulasi juga menjadi aspek penting dalam menghadapi tantangan teknis ini. Regulasi yang ada saat ini perlu diperbarui untuk mengakomodasi kompleksitas teknologi *Deepfake*, termasuk mengatur kewajiban

perusahaan teknologi dalam mencegah dan menangani penyebaran konten *Deepfake*. Dengan regulasi yang lebih jelas dan komprehensif, diharapkan akan tercipta ekosistem yang mendukung upaya penegakan hukum terhadap kejahatan berbasis teknologi.

F. Penguatan Kolaborasi dan Edukasi Publik

Selain aspek penegakan hukum, upaya pencegahan yang dapat dilakukan terhadap dampak negatif dari teknologi *Deepfake* memerlukan pendekatan yang terfokus pada edukasi publik. Edukasi publik tentang bahaya, dampak, dan cara mendeteksi *Deepfake* sangat penting untuk membangun kesadaran dan ketahanan masyarakat. Dalam era digital saat ini yang semakin kompleks, literasi digital menjadi alat yang esensial untuk membantu masyarakat memahami cara mengenali konten manipulatif, balik dalam bentuk gambar, video, maupun audio. Dengan pemahaman yang lebih baik, masyarakat dapat berperan aktif dalam melindungi diri mereka sendiri dari dampak negatif teknologi canggih ini.

Literasi digital tidak hanya berfokus pada penggunaan perangkat teknologi, akan tetapi juga mencakup pemahaman tentang cara kerja teknologi, potensi penyalahgunaan nya, serta langkah- langkah pencegahan. Literasi digital yang efektif dapat mengajarkan masyarakat untuk tidak hanya menjadi konsumen pasif informasi saja, tetapi menjadi pengguna yang kritis terhadap konten yang mereka temui secara online. Dalam konteks teknologi *Deepfake*, literasi digital membantu idividu memahami bagaimana konten manipulatif diciptakan, mengenali tanda-tanda *Deepfake*, dan mengetahui langkah yang harus diambil jika menemukan konten semacam itu.

Sebagai contoh, program literasi digital dapat mengajarkan masyarakat cara menggunakan alat deteksi sederhana yang mampu mengidentifikasi manipulasi visual atau audio. Pelatihan semacam ini juga dapat mencakup pengenalan terhadap teknologi kecerdasan buatan (AI) yang menjadi dasar pembuatan *Deepfake*. Dengan demikian, masyarakat tidak hanya memahami ancaman nya, tetapi juga memiliki keterampilan praktis untuk menghadapinya. Upaya literasi digital tidak dapat dilakukan oleh satu pihak saja. Kolaborasi yang melibatkan pemerintah, lembaga pendidikan, sektor swasta, dan komunitas teknologi diperlukan untuk menciptakan program edukasi yang efektif dan berkelanjutan. Edukasi yang efektif dapat mengurangi risiko penyalahgunaan teknologi dan melindungi masyarakat dari dampak negatif *Deepfake*. Maka, inisiatif edukasi harus melibatkan berbagai pemangku kepentingan untuk memastikan cakupan yang luas dan materi yang relevan. (Yusuf et al, 2024).

Pemerintah dapat mengambil peran dalam menyusun kebijakan digital nasional dan menyediakan dana untuk mendukung program pelatihan di seluruh wilayah. Lembaga pendidikan, seperti sekolah dan universitas, dapat mengintegrasikan literasi digital ke dalam kurikulum mereka, sehingga generasi muda dapat memahami teknologi seperti

Deepfake sejak dini. Dalam menghadapi ancaman yang bersifat global seperti *Deepfake*, kolaborasi internasional menjadi sangat penting. Pemerintah dan lembaga pendidikan dapat bekerja sama dengan komunitas teknologi global untuk mengembangkan alat dan sumber daya yang lebih canggih dalam mendeteksi dan mencegah penyebaran *Deepfake*. Selain itu juga, berbagai pengetahuan dan praktik terbaik dengan negara lain dapat mempercepat upaya mitigasi dampak dari *Deepfake*.

Melalui literasi digital yang efektif, masyarakat tidak hanya lebih siap menghadapi ancaman teknologi canggih seperti *Deepfake*, tetapi menjadi lebih tangguh secara sosial. Ketika masyarakat memiliki pemahaman yang baik tentang teknologi ini, mereka lebih mampu menolak informasi yang salah dan tidak mudah terpengaruh oleh konten manipulatif. Hal ini sangat penting untuk menjaga kepercayaan publik terhadap informasi digital dan mencegah disintegrasi sosial yang disebabkan oleh penyebaran informasi palsu.

4. Kesimpulan

Di Indonesia, regulasi terkait penyebaran konten *Deepfake* masih berada pada tahap awal dan belum mampu menangani kompleksitas ancaman yang ditimbulkan oleh teknologi ini. Ketidakjelasan regulasi ini menciptakan celah hukum yang berpotensi dimanfaatkan oleh pelaku kejahatan untuk menghasilkan dan menyebarkan konten *Deepfake*, baik untuk tujuan pencemaran nama baik, penipuan, maupun eksploitasi seksual. Akibatnya, korban dari kejahatan berbasis *Deepfake* sering kali tidak mendapatkan perlindungan hukum yang memadai, sementara proses penegakan hukum terhambat oleh minimnya pedoman yang jelas dan alat deteksi yang memadai. Maka kesimpulannya, regulasi yang ada saat ini belum cukup untuk melindungi korban atau mencegah penyebaran konten *Deepfake* secara efektif. Oleh karena itu diperlukan langkah strategis dan sistematis untuk memperbarui kerangka hukum dengan menambahkan regulasi yang mengatur mengenai *deepfake* dimana platform digital wajib menyediakan alat pendeteksi *Deepfake* guna melindungi pengguna dari potensi manipulasi , meningkatkan kapasitas teknis, serta memperkuat kolaborasi lintas sektor guna mengatasi tantangan yang ditimbulkan oleh teknologi *Deepfake*.

Berdasarkan kesimpulan diatas, disarankan pemerintah mengambil langkah-langkah strategis dan komprehensif seperti percepatan dan penguatan kerangka regulasi, peningkatan kapasitas penegak hukum, penguatan perlindungan korban, kolaborasi lintas sektor dan internasional serta pengembangan riset dan teknologi.

5. Daftar Pustaka

Agung, A., Hafrida, H., & Erwin, E. (2023). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal Law*, *3*(2), 212–222. https://doi.org/10.22437/pampas.v3i2.23367

Andika, & M. Soemarno. (2023).Masalah Privasi dan Keamanan Data Pribadi pada Penerapan Kecerdasan Buatan. *INNOVATIVE: Journal Of Social Science Research*, *3*, 4917– 4929

Jamaaluddin, D. I., & Sulistyowati, I. (2021). *Buku Ajar Mata Kuliah Kecerdasan Buatan (Artificial Intelligence)*. UMSIDA Press

Muttaqin, M. A., Jaya, A. K., Suryawan, M. A., Gustiana, Z., & Banjarnahor, A. R. (2023). *Implementasi Artificial Intelligence (AI) dalam Kehidupan*. Yayasan Kita Menulis

Mufti, M. W., Ikhsan, M. H., Sani, R., & Fauzan, M. (2024). Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *1*(11).

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara. *Jurnal Usm Law Review*, *7*(2), 603. https://doi.org/10.26623/julr.v7i2.8995

Novera, O., & Z, Y. F. (2024). *Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial*. *10*(2), 460–474.

Respati, A. A., Dewi Setyarini, A., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A.A. (n.d.). *Media Hukum Indonesia (MHI) Analisis Hukum Terhadap Pencegahan Kasus DeepfakeSerta Perlindungan Hukum Terhadap Korban*. *2*(2), 586.https://doi.org/10.5281/zenodo.12508126

Rizki Kurniawan, M., Nabila, T., Khalidy, A., Juniarti Tan, V., Widiyani, H., Hukum Universitas Maritim Raja Ali Haji Abstrak, I., & Kunci, K. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: *Deepfake* Pornografi dan Pencurian Data Pribadi. *Jurnal Ilmiah Wahana Pendidikan*, *10*(10), 534–547.https://doi.org/10.5281/zenodo.11448814

Raharjo, B. (2023). *Teori Etika dalam Kecerdasan Buatan (AI)*. Yayasan Prima Agus Teknik

Syaifudin, P. N. A. (2024). Hukum Dan Teknologi: Dinamika Regulasi Di Era Revolusi Digital. *Kultura Jurnal Ilmu Sosial Dan Humaniora*, *Vol. 2*(No. 9), 376–381. https://jurnal.kolibi.org/index.php/kultura/article/view/2689

Santoso, J. T. (2023). *Kecerdasan Buatan (Artificial Intelligence)*. Yayasan Prima Agus Teknik

Susatyono, J. D. (2021). *Kecerdasan Buatan: Kajian Konsep dan Penerapan*. Yayasan Prima Agus Teknik

Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2022). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi. *Meraja Journal*, *5*(3), 115–137.

Yusuf, K., Frasetyo, M., Gumilar, R. R., & Hosnah, A. U. (2024). Perlindungan Hukum Terhadap Korban Kejahatan Identitas Online Di Indonesia. *Jurnal Ilmu Hukum*, *2*(1), 236. http://jurnal.kolibi.org/index.php/kultura

Peraturan Perundang-undangan

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Conflict of interest statement: The author(s) declares that the research was conducted in the absence of any commercial finance relationship that could be construed as a potential of interest.

UIR Law Review (UIRLRev) is an open access and peer-reviewed journal published by Faculty of Law, Universitas Islam Riau, Indonesia.