Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://jhlg.rewangrencang.com/

ANALISIS PERTANGGUNGJAWABAN PERDATA TERHADAP PENYALAHGUNAAN TEKNOLOGI *ARTIFICIAL INTELLIGENCE (DEEPFAKE)*

CIVIL LIABILITY ANALYSIS FOR THE MISUSE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY (DEEPFAKE)

Nabilatul Alimah Putri, Nabilah Nurmasitha dan Ni Luh Neisya

Fakultas Hukum Universitas Airlangga

Korespondensi Penulis : nabilatul.alimah.putri-2024@fh.unair.ac.id, nabilah.nurmasitha-2024@fh.unair.ac.id, :ni.luh.neisya-2024@fh.unair.ac.id

Citation Structure Recommendation :

Putri, Nabilatul Alimah, Nabilah Nurmasitha dan Ni Luh Neisya. *Analisis Pertanggungjawaban Perdata terhadap Penyalahgunaan Teknologi Artificial Intelligence (Deepfake)*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).

ABSTRAK

Perkembangan teknologi artificial intelligence (deepfake) banyak disalahgunakan untuk memanipulasi wajah milik seseorang menjadi wajah milik orang lainnya sehingga berpotensi untuk disalahgunakan dalam melakukan kejahatan seperti penipuan, penyalahgunaan data pribadi, pemerasan, pornografi dan sabotase politik, dengan berdasarkan hal tersebut penelitian ini bertujuan untuk mengetahui bagaimana pertanggungjawaban perdata terhadap penyalahgunaan teknologi deepfake dan bagaimana tantangan dan solusi dalam penerapan pertanggungjawaban perdata terhadap pelaku penyalahgunaan deepfake.

Dengan tipe penelitian normatif serta menggunakan pendekatan konseptual dan perundang-undangan, dengan menelaah semua undang-undang dan regulasi mengenai pertanggungjawaban perdata penyalahgunaan teknologi deepfake. Hasil penelitian ini menunjukkan bahwa baik penyedia maupun pengguna platform deepfake dapat dimintai pertanggungjawaban atas kelalaian atau kesalahan yang menimbulkan kerugian, hal demikian sebagaimana konsep perbuatan melawan hukum yang diatur dalam Pasal 1365 dan Pasal 1367 KUHPerdata. Kemudian implementasi pertanggungjawaban perdata atas penyalahgunaan deepfake masih menghadapi kompleksitas signifikan. Tantangan tersebut berasal dari aspek teknis, seperti keterbatasan generalisasi model deteksi dan tingginya realisme konten deepfake yang dipicu oleh teknologi deep learning serta aksesibilitas perangkat lunak yang mudah. Terhadap penegakan hukum mengalami kendala dalam mengidentifikasi pelaku, isu yurisdiksi lintas batas, dan kesulitan kuantifikasi kerugian imateriil. Selain itu, terdapat kekosongan hukum spesifik yang secara eksplisit mengatur deepfake, menjadikan pengaturan hukum yang ada bersifat umum dan belum adaptif terhadap karakteristik manipulasi berbasis artificial inttelligence.

Kata Kunci: Penyalahgunaan Teknologi, *Artificial Intelligence Deepfake*, Perbuatan Melawan Hukum

ABSTRACT

The development of artificial intelligence (deepfake) technology has been widely misused to manipulate a person's face into that of another person, potentially leading to its misuse in crimes such as fraud, misuse of personal data, extortion, pornography, and political sabotage. Based on this, this study aims to determine how civil liability applies to the misuse of deepfake technology and what challenges and solutions exist in applying civil liability to those who misuse deepfake technology. Using a normative research approach combined with conceptual and legal frameworks, this study examines all laws and regulations related to civil liability for the misuse of deepfake technology. The results of this study indicate that both providers and users of deepfake platforms can be held liable for negligence or errors that cause harm, as per the concept of unlawful acts regulated in Articles 1365 and 1367 of the Civil Code. However, the implementation of civil liability for deepfake misuse still faces significant complexities. These challenges stem from technical aspects, such as the limitations of detection model generalization and the high realism of deepfake content driven by deep learning technology, as well as the ease of access to software. Enforcement of the law faces obstacles in identifying perpetrators, cross-border jurisdictional issues, and difficulties in quantifying immaterial losses. Additionally, there is a specific legal vacuum that explicitly regulates deepfakes, making existing legal regulations general and not yet adaptive to the characteristics of artificial intelligence-based manipulation.

Keywords: Technology Abuse, Artificial Intelligence Deepfake, Illegal Acts

A. PENDAHULUAN

Perkembangan teknologi telah mengubah peradaban manusia secara menyeluruh. Inovasi digital membuka banyak peluang baru dalam berbagai bidang, mulai dari komunikasi, pendidikan, transportasi, hingga teknologi lainnya. Di era modern saat ini, literasi digital penting bagi masyarakat untuk dapat berpikir cerdas sekaligus waspada dalam menghadapi kemajuan teknologi. Hal ini dikarenakan adanya risiko yang mungkin muncul dari kecanggihan teknologi tersebut. Di satu sisi, teknologi memberikan kemudahan dan bermanfaat positif. Namun, di sisi lain kemajuan ini juga membawa tantangan seperti ketergantungan berlebihan, penyalahgunaan, penyebaran informasi palsu, dan masalah privasi yang dapat menimbulkan efek negatif terhadap masyarakat itu sendiri. Salah satu bentuk teknologi yang berpotensi merugikan individu dan masyarakat adalah Artificial Intelligence (AI).

Perkembangan Artificial Intellegence memunculkan suatu algoritma tertentu yang disebut Deepfake Technology. Deepfake adalah sebuah istilah yang digunakan pada algoritma yang memiliki sistem kerja yang dapat mengubah wajah satu aktor menjadi wajah aktor lain dalam foto dan atau video sehingga menghasilkan photorealistic dalam arti gaya artistik yang merepresentasikan suatu subjek dalam arah yang akurat dan detil, seperti sebuah fotografi. Sehingga belakangan ini, deepfake banyak digunakan untuk memanipulasi fotografi dan videografi untuk memanipulasi wajah milik seseorang menjadi wajah milik orang lainnya dan berpotensi untuk disalahgunakan dalam melakukan kejahatan seperti pornografi, balas dendam, bullying, sabotase politik, pemerasan, bukti video palsu, penipuan, pencurian identitas, dan isu privasi lainnya. Perbuatan pelaku memalsukan penggunaan data pribadi milik seseorang menggunakan teknologi deepfake bertujuan pula untuk mendapatkan keuntungan mengakibatkan kerugian bagi korban, yaitu bocornya data pribadi miliknya.

Perkembangan teknologi yang pesat membutuhkan perkembangan hukum juga demi perlindungan penggunanya. Dalam hukum Indonesia, perlindungan pribadi tertuang dalam Pasal 28G ayat (1) Undang-Undang Dasar Tahun 1945 yang menyatakan "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Melihat banyaknya penyalahgunaan informasi pribadi, maka dibutuhkan perlindungan dan jaminan keselamatan informasi setiap pribadi. Selain itu, dalam pembukaan Undan-Undang Dasar Tahun 1945, khususnya alinea keempat dinyatakan bahwa "Pemerintah Negara Indonesia mempunyai tanggung jawab konstitusional untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial.

Aplikasi deepfake kerap disalahgunakan untuk mengubah wajah seseorang yang satu dengan orang lain dalam bentuk video atau gambar dengan tingkat kualitas seperti asli atau nyata. Permasalahan ini memunculkan berbagai dampak terhadap korban karena gambar atau video mereka meskipun hasil dari buatan AI.

Hal tersebut tetap berdampak negatif karena dapat memunculkan dampak psikologis kepada korban akibat rusaknya citra korban di masyarakat, akibat tidak terjaganya privasi dan rasa aman bagi korban. Di media sosial, deepfake sedang banyak diperbincangkan karena maraknya kasus dimana wajah seseorang disalahgunakan dalam bentuk gambar ataupun video. Terlebih lagi dalam hal ini yang sering menjadi korban kejahatan penyalahgunaan teknologi tersebut adalah perempuan dan tokoh-tokoh penting. Hal ini menunjukkan betapa buruknya kejahatan penyalahgunaan teknologi saat ini. Tanpa perlu mengenal korban secara langsung, pelaku dapat memanfaatkan teknologi deepfake selama memiliki rekaman gambar atau video korban.

Mengingat penggunaan kecerdasan buatan atau artificial intelligence terlebih pada deepfake tersebut telah berkembang pesat dan diaplikasikan secara luas baik di sektor publik maupun privat. Kondisi tersebut memerlukan analisis komprehensif terkait bentuk pertanggungjawaban perdata atas kerugian yang ditimbulkan oleh Artificial Intelligence (deepfake). Urgensi topik ini terletak pada kontribusinya terhadap pengembangan doktrin hukum perdata dan perumusan kebijakan yang relevan. Oleh karena itu, diperlukan kerangka regulasi yang dinamis dan adaptif guna mengantisipasi serta mengelola potensi risiko di masa mendatang. Berdasarkan latar belakang permasalahan tersebut adapun dapat ditentukan topik permasalahan dalam penelitian ini yaitu : 1) Pertanggungjawaban perdata terhadap penyalahgunaan teknologi deepfake, 2) Bagaimana tantangan dan solusi dalam penerapan pertanggungjawaban terhadap pelaku penyalahgunaan deepfake. Sehingga penelitian ini bertujuan untuk memberikan pemahaman kepada korban penyalahgunaan teknologi deepfake dalam ranah hukum keperdataan dan memberikan pemahaman bagaimana tantangan dan solusi dalam penanganan pelaku penyalahgunaan deepfake, serta dalam penelitian ini juga bertujuan untuk memberikan saran kepada pemerintah agar membentuk regulasi khusus terkait pertanggungjawaban penyalahgunaan teknologi deepfake dalam ranah hukum perdata di masa yang akan datang.

B. PEMBAHASAN

1. Pengaturan Hukum Pertanggungjawaban Perdata terhadap Pelaku Penyalahgunaan Deepfake

Salah satu karya Artificial Intelligence (AI) yang menjadi sorotan adalah deepfake. Deepfake merujuk pada penggabungan teknologi deep learning dengan tujuan menciptakan konten palsu. Deep learning, pada dasarnya, adalah teknik yang digunakan untuk melatih AI agar dapat mengeksekusi suatu tugas tertentu. Deepfake adalah Istilah yang digunakan untuk algoritma tersebut adalah teknik pemrosesan video yang memungkinkan pengguna untuk mengganti wajah satu aktor dengan wajah aktor lain dalam video dengan tingkat keaslian gambar yang tinggi yakni meniru objek visual yang nyata. Selain dalam bentuk video, teknologi deepfake juga dapat digunakan untuk merekayasa gambar. Pada tahun 2017, istilah "deepfake" mulai mendapatkan perhatian luas berkat seorang pengguna Reddit yang memanfaatkan Generative Adversarial Networks (GAN), Sebuah prosedur pembelajaran mesin, serta TensorFlow, sebuah perangkat lunak yang dibuat oleh Google untuk memperdalam pemahaman dan pembelajaran mesin, Semakin banyak sampel gambar wajah dan rekaman suara yang tersedia dari subjek sumber, semakin realistis dan autentik kontennya. Kehadiran teknologi ini telah menimbulkan kekhawatiran yang signifikan terkait dengan potensi dan dampak negatif dari deepfake, yang memiliki kemampuan untuk mengelabui penglihatan manusia.[1]

Contoh aplikasi yang memakai teknologi deepfake yang mudah diakses bebas adalah aplikasi MyHeritage, FaceApp,0020ataupun Deepfake Studio yang secara fungsinya kurang lebih sama, yakni alat bantu untuk merekonstruksi wajah seseorang kemudian menerapkannya secara akurat terhadap gambar atau video yang berbeda. Kondisi yang demikian pun telah terlihat secara nyata ancaman bahayanya jika merujuk pada siaran pers Kemenkominfo tertanggal 16 November 2023, berdasarkan laporan yang dipublikasikan Home Security Heroes, terdapat sebanyak 95.820 video deepfake yang tersebar secara global pada tahun 2023.

[1] Silvia Mah Arani Iskandar Putri dkk., *Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum*, Jurnal Hukum Legalita, Vol.6, No.2 (2024), p.85.

Menelaah data sebelumnya juga, berdasarkan hasil survei yang telah dilakukan oleh The AI Firm Deeptrace pada tahun 2019 lalu, ditemukan sebuah data bahwa sebanyak 96% video yang dibuat oleh deepfake adalah bermuatan pornografi.[2]

Pengaturan hukum terhadap penyalahgunaan AI deepfake di Indonesia sejatinya belum diatur secara eksplisit sekalipun pengaturan hukum yang sudah ada namun belum mencakup seluruh aspek terkait penyalahgunaan deepfake, sehingga peristiwa tersebut mungkin saja akan terulang lagi di masa mendatang dan pelaku deepfake akan melenggang bebas memainkan dialog tokoh-tokoh penting karena tidak adanya ketegasan dari Undang-Undang. Keberadaan deepfake dianggap sebagai kejahatan cyber dikarenakan hasil konten video yang diubah telah disebar melalui internet dan kemudian terciptalah peristiwa-peristiwa yang tidak ada atau tidak benar-benar terjadi. Sehingga deepfake banyak digunakan untuk tujuan kejahatan seperti menyesatkan masyarakat dengan menyebarkan informasi palsu atau propaganda. Sebagai contoh lainnya terdapat video deepfake yang menampilkan pemimpin dunia atau orang terkenal lainnya yang mengatakan sesuatu yang tidak mereka katakan, sehingga hal tersebut mengubah opini publik.

Meskipun kecerdasan buatan AI memiliki kemampuan yang sangat kuat memproses data dan mengenali pola yang kompleks, AI hanya dapat beroperasi berdasarkan instruksi yang dibuat oleh orang. Dalam hal ini tentu terdapat risiko hilangnya informasi yang berguna dan bermanfaat sebagai konsekuensi dari perantara penyedia layanan internet yang menerapkan filter Al pada rentang informasi yang terlalu sempit untuk menghindari penalti. Oleh karena itu, kecerdasan buatan tidak memiliki pemahaman inheren tentang nilai-nilai moral manusia, sehingga tidak mampu menetapkan apakah informasi yang diproses sesuai dengan standar, undang-undang, atau etika. Akibatnya, orang-orang, termasuk pengembang AI, bertanggungjawab atas penggunaan AI secara etis, hukum, dan moral. Hingga saat ini, di Indonesia, belum ada undang-undang yang secara khusus dan rinci mengatur penggunaan kecerdasan buatan AI. Peraturan yang telah ada saat ini mengatasi AI sebagai agen elektronik, yakni perangkat elektronik yang dapat menjalankan tugas-tugas otomatis terkait informasi elektronik. Akan tetapi,

[2] Fasa Muhamad Hapid, dkk. *Penerapan Asas Geen Straf Zonder Schuld dalam Penindakan terhadap Kejahatan Penyalahgunaan Teknologi Deepfake*, Jurnal USM Law Review, Vol.7, No.3 (2024), p.1160.

peraturan tersebut tidak sepenuhnya menyentuh situasi yang lebih dalam terkait dengan etika, privasi, dan konsekuensi sosial dari penggunaan AI. Kekurangan kerangka dasar hukum yang jelas dan spesifik untuk AI bisa menimbulkan keraguan seputar tanggung jawab, etika, dan konsekuensi sosial dari teknologi AI.

Kemajuan sistem internet dan kemudahan pertukaran data yang semakin masif kemudian menyebabkan kerentanan terjadinya intervensi terhadap data pribadi yang merupakan privasi. Data pribadi seseorang menjadi mudah untuk disebarluaskan dan dibagikan secara semena-mena ke ruang yang dapat diakses publik tanpa sepengetahuan dan seizin dari pemilik data.[3] Oleh karena itu diperlukannya pengaturan terkait perlindungan data pribadi. Perlindungan privasi dan data pribadi disebutkan dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28G yang berbunyi: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Dalam lingkup internasional, Deklarasi Universal Hak Asasi Manusia/Universal Declaration of Human Rights (DUHAM/UDHR) telah mengatur terkait privasi dalam Pasal 12 yang menyatakan, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks." Pasal tersebut menyatakan bahwa seseorang memiliki hak atas privasinya, keluarganya, tempat tinggal, korespondensi, dan kehormatan dan reputasinya. Seseorang juga memiliki hak untuk memperoleh perlindungan hukum terhadap setiap pelanggaran yang terjadi atas mereka.[4]

Adapun ketentuan yang terdapat di dalam peraturan perundang-undangan yang mengatur mengenai perlindungan data pribadi secara umum seperti UUD NRI 1945, UU 39/1999 tentang HAM, dan UU 19/2016 tentang ITE ternyata belum satupun yang mengatur atau sekedar menyinggung mengenai penyalahgunaan dan pemalsuan data pribadi menggunakan teknologi Artificial Intelligence deepfake.

---

[3] Siti Yuniarti, *Perlindungan Hukum Data Pribadi di Indonesia*, Jurnal BECOSS, Vol.1, No.1 (2019), p.148.

[4] Alifia Jasmine, Benny Djaja dan Maman Sudirman, *Tanggung Jawab Notaris dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Jurnal Ilmu Hukum, Humaniora dan Politik, Vol.5, No.1 (November 2024), p.653–62.

Dalam peraturan perundang-undangan tersebut hanya menyebutkan hak atas perlindungan data pribadi merupakan hak setiap orang, kewajiban menjaga kerahasiaan data pibadi, atau keharusan memperoleh ijin dari pemilik data pribadi sebelum menggunakannya. Peraturan perundang-undangan tersebut tidak menjelaskan apabila data pribadi yang merupakan hak setiap orang tersebut disalahgunakan dengan cara-cara tertentu yaitu menggunakan teknologi AI deepfake seperti dalam kasus pemalsuan data pribadi menggunakan AI deepfake.

Ketika kecerdasan buatan melakukan otomatisasi dalam pengolahan data, hal ini dapat dianggap sebagai sebuah "Entitas Elektronik" sesuai dengan peraturan di Indonesia. Pasal 1 angka 8 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menggambarkan agen elektronik sebagai : Agen Elektronik adalah perangkat dalam sistem elektronik yang otomatis melakukan tindakan terhadap informasi elektronik tertentu yang dioperasikan oleh manusia. Kata "otomatis", berarti bekerja sendiri menurut KBBI, digunakan sebagai dasar untuk menyamakan karakteristik AI dengan Agen Elektronik. Oleh karena itu, dapat diasumsikan bahwa peraturan tentang "Agen Elektronik" dapat juga berlaku untuk teknologi kecerdasan buatan yang memiliki karakteristik yang sama.

Meskipun tidak secara eksplisit mengatur kecerdasan buatan, UU ITE telah memberikan landasan hukum untuk mengatur teknologi kecerdasan buatan, terutama dalam konteks deepfake.[5] Serangkaian perbuatan oleh pelaku yang memalsukan data pribadi milik korban dengan menggunakan teknologi deepfake termasuk dalam perbuatan yang dilarang oleh undang-undang sebagaimana disebukan dalam Pasal 35 UU ITE “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik”. Pelanggaran terhadap Pasal tersebut diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah).

[5] Sabrina Nur Syahirah, *Tinjauan Yuridis terhadap Penggunaan Teknologi Deepfake untuk Pornografi Melalui Artificial Intelligence (AI) di Indonesia*, Jurnal Inovasi Hukum dan Kebijakan, Vol.6, No.1 (2025), p.201.

Meskipun serangkaian perbuatan pemalsuan yang dilakukan pelaku menggunakan teknologi deepfake belum diatur secara khusus melalui peraturan perundang-undangan, namun berdasarkan ketentuan yang diatur dalam Pasal 35 UU ITE tersebut dapat mengaitkan perbuatan pemalsuan yang dilakukan pelaku dengan jaminan kepastian hukum terhadap korban pemalsuan data pribadi menggunakan teknologi deeepfake. Perlindungan tersebut merupakan hak bagi korban untuk dilindungi data/informasi pribadi miliknya dari perubahan atau pengerusakan sehingga data/informasi yang telah dimanipulasi dianggap sebagai data asli dan autentik baik digunakan untuk tujuan apapun. Sehingga apabila hak yang dimiliki tersebut dilanggar, maka korban dapat menyelesaikan masalah tersebut melalui upaya hukum dengan mengajukan gugatan kepada pengadilan. Upaya hukum gugatan ke pengadilan diajukan dengan tujuan untuk memulihkan keadaan dan mengembalikan kerugian yang telah diderita. Pengajuan gugatan ke pengadilan bukan hanya untuk menuntut pelaku pemalsuan data pribadi korban dengan menggunakan teknologi deepfake, serta pihak lain yang tidak memiliki hubungan hukum dengan pemilik data pribadi yang telah menyebarluaskan data pribadi milik korban

Pasal 26 ayat (1) dan (2) UU ITE menyebutkan bahwa: (1) “Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.” (2) “Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-undang ini”. Hak yang dimiliki setiap orang sebagai pemilik data pribadi untuk selalu menjaga kerahasiaan data pribadinya berdasarkan ketentuan Pasal 26 ayat (1) dan (2) UU ITE tersebut apabila data pribadi miliknya disalahgunakan atau disebar luas oleh pihak lain, maka pemilik data pribadi yang datanya disalahgunakan dapat mengajukan gugatan perdata disertai ganti kerugian ke pengadilan. Ketentuan yang diatur dalam pasal tersebut merupakan perlindungan yang diberikan terhadap data pribadi seseorang secara umum, yaitu dalam arti terhadap setiap kegiatan transaksi elektronik yang menggunakan data pribadi seseorang harus dengan seizin dari pemilik data pribadi tersebut, hal ini dilakukan sebagai bentuk menjaga dan melindungi data pribadi.

Dengan ketentuan tersebut, maka setiap orang mempunyai hak untuk menyimpan, merawat, dan menjaga kerahasiaan data miliknya agar tetap bersifat pribadi.[6]

Konsep tanggung jawab hukum berhubungan dengan konsep kewajiban hukum, bahwa seseorang bertanggung jawab secara hukum atas perbuatan tertentu.[7] Menurut Hans Kelsen dalam teorinya tentang tanggung jawab hukum menyatakan bahwa: "seseorang bertanggung jawab secara hukum atas suatu perbuatan tertentu atau bahwa dia memikul tanggung jawab hukum, subyek berarti bahwa dia bertanggung jawab atas suatu sanksi dalam hal perbuatan yang bertentangan.[8] Menurut, Hans Kelsen membagi mengenai tanggung jawab terdiri dari: 1. Pertanggungjawaban individu yaitu seorang individu bertanggung jawab terhadap pelanggaran yang dilakukannya sendiri; 2. Pertanggungjawaban kolektif berarti bahwa seorang individu bertanggung jawab atas suatu pelanggaran yang dilakukan oleh orang lain; 3. Pertanggungjawaban berdasarkan kesalahan yang berarti bahwa seorang individu bertanggung jawab atas pelanggaran yang dilakukannya karena sengaja dan diperkirakan dengan tujuan menimbulkan kerugian; 4. Pertanggungjawaban mutlak yang berarti bahwa seorang individu bertanggung jawab atas pelanggaran yang dilakukannya karena tidak sengaja dan tidak diperkirakan.[9]

Secara umum pertanggungjawaban dapat dilimpahkan ke subjek hukum yang bertindak melawan hukum. Seperti yang telah dijelaskan sebelumnya, pertanggungjawaban itu timbul atas kesalahan yang dilakukan oleh subjek hukum dan menimbulkan kerugian. Pertanggungjawaban lekat pada subjek hukum atas kerugian yang ditimbulkan sendiri. Pasal 1365 KUHPerdata menjadi rumusan umum yang mengatur ketentuan tentang perbuatan melawan hukum. Pasal ini menyebutkan bahwa setiap perbuatan yang bertentangan dengan hukum dan menyebabkan orang lain menjadi merugi, maka harus terdapat ganti kerugian.

---

[6] Ni Nyoman Ari Diah Nurmantani dan Nyoman A. Martana, *Perlindungan Hukum terhadap Data Pribadi Peminjam dalam Layanan Aplikasi Pinjaman Online*, Journal Ilmu Hukum, Vol.1, No.1 (2019), p.5-6.

[7] Shinta Titik Triwulan, *Perlindungan Hukum Bagi Pasien*, Prestasi Pustaka, Jakarta, 2010, p.48.

[8] Hans Kelsen, *General Theory Of Law and State, Teori Umum Hukum dan Negara, Dasar-Dasar Ilmu Hukum Normatif sebagai Ilmu Hukum Deskriptif Empirik*, terj. Soemardi, BEE Media Indonesia, Jakarta, 2007, p.81.

[9] Raisul Mutaqien Hans Kelsen, *Teori Hukum Murni Nuansa & Nusa Media*, Nuansa & Nusa Media, Bandung, 2006, p.140.

Pasal 1365 ini hanya berlaku bagi kerugian yang timbul sebagai akibat kesalahan subjek hukum itu sendiri. Apabila Artificial Intelligence diberikan pertanggungjawaban ini tidaklah tepat karena Artificial Intelligence bukanlah subjek hukum yang diakui secara yuridis. Apabila "sesuatu" mempunyai hak dan kewajiban sama seperti manusia sebagai subjek hukum, maka "sesuatu" yang mempunyai hak dan kewajiban termasuk dalam subjek hukum yang termasuk dalam golongan badan hukum.[10] Namun Artificial Intelligence tidaklah dapat disandangi hak dan kewajiban dikarenakan karakternya yang bergantung pada manusia.

Pengertian perbuatan dalam perbuatan melawan hukum memiliki arti perbuatan aktif maupun pasif, dengan kata lain ketidakaktifan dalam bertindak oleh seseorang dapat dikategorikan sebagai perbuatan dan apabila perbuatan tidak aktif tersebut kemudian melanggar hukum maka dapat dikategorikan sebagai perbuatan melawan hukum. Perbuatan aktif maupun pasif yang menimbulkan kerugian bagi korban tidak hanya yang bersifat materiel, melainkan juga dapat bersifat imateriel. Oleh karena itu, pihak yang terlanggar hak dan kepentingannya, tidak hanya dapat meminta ganti kerugian berwujud uang, melainkan juga dapat meminta agar dilakukan pengembalian pada keadaan semula atas kerugian yang dialaminya. Terdapat beberapa bentuk permintaan ganti kerugian yang dapat diajukan di antaranya :[11] berupa pemberian uang; pengembalian ke keadaan awal; mengaku bahwa perbuatannya merupakan suatu perbuatan yang bertentangan dengan hukum; permintaan agar tidak berbuat; menghilangkan sesuatu yang timbul dari perbuatan melawan hukum; atau dilakukan pengumuman dari keputusan hasil tuntutan.

Artificial Intelligence tidak dapat melakukan perbuatan hukum secara mandiri. Bahkan hingga saat ini Indonesia tidak memberikan legitimasi terhadap Artificial Intelligence yang dianggap sebagai subjek hukum. Oleh karena itu, Artificial Intelligence yang menimbulkan kerugian tidak dapat dikenakan Pasal 1365 KUHPerdata karena Artificial Intelligence bukanlah subjek hukum yang dapat dimintakan pertanggungjawaban. Namun pertanggungjawaban tidak hanya dibebankan atas kerugian yang ditimbulkan secara langsung akibat dirinya sendiri,

[10] M. Yahya Harahap, *Hukum Perseroan Terbatas*, Sinar Grafika, Jakarta, 2016, p.53.
[11] M.A. Moegni Djojodirdjo, *Perbuatan Melawan Hukum*, Pradnya Paramita, Jakarta, 1976, p.102.

melainkan dapat dibebankan kepada seseorang atas kerugian yang timbul akibat perbuatan orang yang ada dalam tanggungannya atau barang dalam pengawasannya. Pertanggungjawaban terhadap kesalahan yang timbul dari perbuatan si tanggungannya atau barang atau hewan peliharaannya yang berada dalam pengawasannya merupakan tanggungjawab tanpa kesalahan atau yang biasa dikenal dengan tanggungjawab mutlak.[12]

Perihal tanggungjawab mutlak ini dimuat dalam Pasal 1367 ayat (1) dan (3) KUHPerdata "(1) Seseorang tidak saja bertanggung jawab untuk kerugian yang disebabkan perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan perbuatan orang-orang yang menjadi tanggungjawabnya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya." dan (3) Majikan-majikan dan orang yang mengangkat orang lain untuk mewakili urusan-urusan mereka adalah bertanggung jawab tentang kerugian yang diterbitkan oleh pelayan-pelayan atau bawahan-bawahan mereka di dalam melakukan pekerjaan untuk mana orang-orang ini dipakainya". Penyalahgunaan deepfake merupakan pelanggaran hukum yang merugikan orang lain, sehingga pelaku harus bertanggung jawab atas kerugian yang ditimbulkan.[13]

Secara umum, pertanggungjawaban hukum berpusat pada subjek hukum yang melakukan perbuatan melawan hukum dan menimbulkan kerugian, sebagaimana diatur dalam Pasal 1365 KUHPerdata. Pasal ini menegaskan kewajiban ganti rugi bagi setiap perbuatan yang bertentangan dengan hukum dan menyebabkan kerugian, baik melalui tindakan aktif maupun pasif, yang dapat bersifat materiil maupun imateriil. Namun, penerapan Pasal 1365 KUHPerdata secara langsung kepada Artificial Intelligence (AI), termasuk deepfake, tidaklah tepat karena AI tidak diakui sebagai subjek hukum yuridis yang memiliki hak dan kewajiban layaknya manusia atau badan hukum. Karakteristik AI yang bergantung pada instruksi manusia menghalanginya untuk melakukan perbuatan hukum secara mandiri. Meskipun demikian, prinsip pertanggungjawaban dapat diperluas.

---

[12] Munir Fuady, *Perbuatan Melawan Hukum Pendekatan Kontemporer*, Penerbit Citra Aditya Bakti, Bandung, 2018, p.173.

[13] M. Ariq Abir Jufri dan Akbar Kurnia, *Aspek Hukum Internasional dalam Pemanfaatan Deepfake Technology terhadap Perlindungan Data Pribadi*, Uti Possidetis: Journal of International Law, Vol.2, No.1 (2021), p.52-53.

AI (deepfake) dapat dianalogikan sebagai "pekerja" atau "barang/pihak yang dalam pengawasan", memungkinkan pembebanan tanggung jawab kepada pemiliknya sebagai "pemberi kerja" atau pihak yang bertanggung jawab atas pengawasan. Konsep ini sejalan dengan pertanggungjawaban mutlak (strict liability) yang diatur dalam Pasal 1367 ayat (1) dan (3) KUHPerdata. Pasal ini memungkinkan seseorang bertanggung jawab atas kerugian yang disebabkan oleh perbuatan orang lain yang berada dalam tanggungannya atau barang/pihak yang berada di bawah pengawasannya. Oleh karena itu, dalam konteks penyalahgunaan deepfake, meskipun AI tidak dapat dipertanggungjawabkan secara independen, penyedia maupun pengguna platform AI (deepfake) dapat dimintai pertanggungjawaban atas kelalaian atau kesalahan yang menimbulkan kerugian, berdasarkan interpretasi luas dari perbuatan melawan hukum (Pasal 1365 KUHPerdata) dan prinsip pertanggungjawaban mutlak (Pasal 1367 KUHPerdata) yang menekankan keterlibatan dan pengawasan manusia.

2. Tantangan dan Solusi Dalam Penerapan Pertanggungjawaban Perdata Terhadap Pelaku Penyalahgunaan Deepfake

Perkembangan teknologi deepfake dalam era AI telah membawa dampak signifikan di berbagai bidang. Dalam industri film, deepfake digunakan untuk meningkatkan produksi efek visual (VFX), memungkinkan penciptaan adegan yang lebih realistis dan kreatif.[14] Selain itu, deepfake juga telah menemukan aplikasi dalam bidang pemasaran, komunikasi politik, dan media, di mana ia dapat digunakan untuk membuat konten yang lebih menarik dan personal.[15] Namun, kemudahan pembuatan deepfake juga menimbulkan ancaman terhadap privasi dan keamanan, karena dapat digunakan untuk menciptakan berita palsu atau merusak reputasi individu.[16]

---

[14] Hardeep Singh dkk., *Deepfake as an Artificial Intelligence Tool for VFX Films*, 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2023, p.1–5.

[15] Büşra Kiliç dan Mehmet Emin Kahraman, *Current Usage Areas of Deepfake Applications with Artificial Intelligence Technology*, İletişim ve Toplum Araştırmaları Dergisi, Vol.3, No.1 (2023). https://doi.org/10.59534/jcss.1358318.

[16] Jayanta Kumar Panda dam Rajnandini Panigrahy, *Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity's Deepfakes News*, ShodhKosh: Journal of Visual and Performing Arts, Vol.4, No.2 (2023), https://doi.org/10.29121/shodhkosh.v4.i2.2023.2268.

Di satu sisi, AI membantu aparat penegak hukum dalam mengidentifikasi pola kejahatan, memprediksi tindakan kriminal, dan meningkatkan efisiensi penyelidikan. Namun, di sisi lain, AI juga digunakan oleh pelaku kejahatan untuk melakukan serangan siber yang lebih canggih, seperti serangan phishing berbasis AI, deepfake, dan ransomware yang menggunakan algoritma pembelajaran mesin untuk menghindari deteksi. Penggunaan AI dalam cybercrime menimbulkan sejumlah tantangan hukum yang kompleks.

Berdasarkan teori schutznorm, untuk menuntut tanggungjawab dari pelaku tindakan melanggar hukum, bukan hanya cukup dengan menunjukkan keterkaitan kausal antara tindakan dan kerugian, tetapi juga harus membuktikan bahwa aturan yang dilanggar memang diciptakan untuk melindungi (schutz) kepentingan korban. Meskipun dasar gugatan dan akibat hukum dari perbuatan melawan hukum terlihat jelas, ada beberapa keterbatasan dan pertimbangan yang perlu dipertimbangkan. Dalam beberapa situasi, pertimbangan etika, kepentingan umum, dan kerumitan kasus dapat mempengaruhi bagaimana hukum diterapkan. Oleh karena itu, perlindungan hukum terhadap perbuatan melawan hukum haruslah bersifat komprehensif dan cermat, dengan mempertimbangkan berbagai faktor yang berkaitan.[17] AI memiliki kemampuan untuk belajar dan beradaptasi dengan cepat, tetapi tidak memiliki kapasitas moral atau etika. Dalam tangan yang salah, AI dapat digunakan untuk tujuan yang merugikan, seperti menciptakan konten palsu (deepfake) yang dapat merusak reputasi seseorang atau bahkan menimbulkan kekacauan sosial. Pada saat yang sama, penggunaan AI oleh aparat penegak hukum juga harus dilakukan dengan hati-hati untuk menghindari pelanggaran terhadap hak asasi manusia, seperti hak privasi dan kebebasan berekspresi.[18]

Meskipun Undang-Undang Pelindungan Data Pribadi (UU PDP), dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah menyediakan landasan hukum untuk mengatasi kasus penyalahgunaan artificial intelligence deepfake, implementasinya masih menghadapi beberapa tantangan substantif.

---

[17] Gisni Halipah, dkk., *Tinjauan Yuridis Konsep Perbuatan Melawan Hukum dalam Konteks Hukum Perdata*, Jurnal Serambi Hukum, Vol.16, No.1 (2023), p.142.

[18] D T Rachmadie, *Regulasi Penyimpangan Artificial Intelligence pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016*, Jurnal Hukum Pidana Dan Penanggulangan Kejahatan, Vol.9, No.2 (2016), p.128–36.

Salah satu tantangan utama adalah kemampuan generalisasi dari model deteksi deepfake. Banyak model deteksi yang ada saat ini dilatih untuk mengenali jenis deepfake tertentu, sehingga kesulitan dalam mendeteksi deepfake yang dihasilkan dengan teknik yang berbeda. Selain itu, deteksi deepfake di dunia nyata sering kali menghadapi kesulitan seperti pengelolaan video dengan banyak orang dalam satu adegan atau pengenalan gerakan wajah yang bergerak mendekati atau menjauhi kamera.[19] Tantangan lain dalam mendeteksi deepfake adalah tingkat realisme yang tinggi dari konten yang dihasilkan. Teknologi deep learning yang digunakan untuk membuat deepfake telah mencapai tingkat realisme yang sangat tinggi, sehingga sulit bagi manusia untuk membedakan antara konten palsu dan asli hanya dengan mata telanjang. Hal ini diperparah dengan ketersediaan perangkat lunak yang dapat diakses secara bebas di internet, memungkinkan individu tanpa keahlian khusus untuk membuat gambar dan video palsu yang sangat realistis. Oleh karena itu, diperlukan alat otomatis yang mampu mendeteksi konten multimedia palsu dan mencegah penyebaran informasi palsu yang berbahaya.[20]

Penegakan hukum seringkali terhambat oleh kesulitan dalam mengidentifikasi pelaku, terutama karena adanya anonimitas daring dan keberadaan pelaku di luar yurisdiksi Indonesia. Kemudian adanya kerugian immateriil yang sulit diukur baik dampak seperti halnya pencemaran nama baik, gangguan psikologis dan kerugian reputasi yang sulit dikuantifikasi secara pasti dalam konteks ganti rugi perdata. Di samping tantangan implementasi, terdapat kekosongan hukum spesifik yang secara eksplisit mengatur penggunaan Artificial intelligence deepfake di Indonesia. UU PDP dan UU ITE masih bersifat umum dan belum secara rinci mengakomodasi isu manipulasi foto dan video berbasis AI deepfake. Penyalahgunaan teknologi deepfake dalam ruang digital menghadirkan tantangan signifikan dalam sistem hukum perdata Indonesia, khususnya dalam membuktikan unsur kesalahan dan menetapkan pihak yang bertanggung jawab.

Kompleksitas tersebut disebabkan oleh karakteristik deepfake yang dapat dengan mudah menyamarkan identitas pelaku, menyebar lintas platform digital,

[19] Andrea Coccomini, Marco Bertini dan Alberto Del Bimbo, *Deepfake Detection: Challenges and Solutions*, Journal of Imaging, Vol.9, No.1 (2023), p.688–89.
[20] L Verdoliva, *Media Forensics and DeepFakes: An Overview*, IEEE Journal of Selected Topics in Signal Processing, Vol.14, No.5 (2020), p.910–32.

serta menimbulkan kerugian yang bersifat immateriil. Untuk menjawab tantangan ini, diperlukan pendekatan hukum yang progresif dan adaptif terhadap perkembangan teknologi. Secara teoritik, pertanggungjawaban perdata atas penyalahgunaan deepfake dapat dianalisis melalui teori perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 KUH Perdata. Namun, untuk konteks teknologi modern, teori ini perlu dilengkapi dengan pendekatan lain seperti teori strict liability, yakni pertanggungjawaban tanpa harus membuktikan unsur kesalahan, serta teori alokasi risiko, yang menempatkan tanggung jawab pada pihak yang secara teknis memiliki kapasitas pengendalian seperti platform digital.

Salah satu solusi yang paling mendesak adalah reformasi regulasi. Saat ini, hukum positif Indonesia belum memiliki pengaturan khusus mengenai konten manipulatif berbasis kecerdasan buatan. Oleh sebab itu, diperlukan pembentukan norma lex specialis yang tidak hanya mendefinisikan perbuatan melawan hukum dalam konteks digital, tetapi juga mengakomodasi jenis kerugian baru seperti kerusakan reputasi daring, manipulasi identitas, hingga gangguan psikologis yang dialami korban. Selain itu, perlu ditegaskan tanggung jawab platform digital. Dalam banyak kasus, konten deepfake tersebar melalui media sosial dan situs berbagi video tanpa pengawasan yang memadai. Dengan menerapkan prinsip strict liability terhadap platform yang lalai melakukan moderasi, korban akan lebih mudah mendapatkan pemulihan melalui mekanisme gugatan perdata.

Peningkatan literasi hukum dan digital menjadi instrumen penting untuk memperkuat posisi masyarakat sebagai pengguna teknologi. Pengetahuan mengenai hak-hak hukum, jalur pengaduan, dan bentuk-bentuk penyalahgunaan deepfake harus ditanamkan sejak dini, baik melalui pendidikan formal maupun kampanye publik. Tidak kalah penting, kerja sama internasional menjadi tulang punggung keberhasilan penegakan hukum lintas batas. Mengingat pelaku deepfake kerap kali beroperasi dari luar negeri, maka dibutuhkan perjanjian kerja sama antarnegara dalam rangka pertukaran informasi digital, pelacakan siber, hingga ekstradisi pelaku lintas yurisdiksi. Dengan demikian, pemenuhan pertanggungjawaban perdata dalam penyalahgunaan deepfake menuntut pendekatan holistik antara pembaruan hukum secara nasional, penguatan peran aktor digital, dan dengan sinergi global di dalam menanggulangi kejahatan siber.

Dalam perspektif hukum, hal ini juga sejalan dengan semangat perlindungan hak asasi manusia, khususnya hak atas privasi dan kehormatan pribadi yang dijamin dalam sistem hukum nasional maupun instrumen internasional.

3. Langkah Pencegahan terhadap Penyalahgunaan Teknologi *Artificial Intelligence* (*Deepfake*)

Dengan kemampuan deep learning yang dimiliki, AI dirancang mampu mempelajari data yang kompleks dan abstrak hingga merubahnya menjadi berbagai hal dan aktivitas pekerjaan yang biasanya dilakukan manusia seperti pemahaman bahasa, pengenalan pola, pengumpulan data, dan lain sebagainya yang dinilai menyerupai bahkan lebih baik dari kemampuan manusia.[21] Namun, masifnya perkembangan AI tidak hanya memberikan peluang kemudahan dalam membantu manusia, tetapi juga menimbulkan kekhawatiran dari adanya ancaman dan kerugian yang ditimbulkan oleh penggunaan teknologi AI kepada masyarakat. Kekhawatiran tersebut berangkat dari AI yang menggunakan data-data untuk pemrosesannya, dimana data tersebut mungkin mengancam hak privasi dan keamanan data pribadi masyarakat. Salah satu jenis AI yang saat ini menuai banyak perdebatan adalah deepfake, yang merupakan jenis AI yang merujuk pada teknologi yang dikembangkan untuk pembuatan video, audio, atau gambar palsu.[22]

Dalam konteks hukum privasi, teori privacy as control yang dikembangkan oleh Alan Westin menegaskan individu memiliki hak untuk mengontrol informasi pribadinya dan menentukan sejauh mana informasi tersebut dapat diakses oleh pihak lain. Namun, dengan berkembangnya deepfake yang mampu merekayasa data biometrik seseorang seperti wajah dan suara tanpa izin, prinsip dasar kontrol atas informasi pribadi menjadi semakin terancam. Deepfake dapat digunakan untuk membuat konten yang menyesatkan atau bahkan merusak reputasi seseorang tanpa persetujuan, yang secara langsung melanggar hak privasi individu sebagaimana dijelaskan dalam teori Westin. Penyalahgunaan deepfake juga bertentangan dengan teori privacy as dignity, yang menekankan bahwa privasi berkaitan erat dengan martabat individu. Teori ini sendiri banyak dianut dalam sistem hukum di Eropa,

[21] Ranti Fauza Mayana, *Legal Issues of Artifi cial Intelligence Generated Works: Challenges on Indonesian Copyright Law*, Law Reform, Vol.20, No.1 (2024), p.55.
[22] Rendi Syaputra, *Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake Melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia*, Respublica, Vol.24, No.01 (2024), p.2.

terutama dalam General Data Protection Regulation (GDPR) yang menempatkan perlindungan data pribadi sebagai bagian dari perlindungan hak asasi manusia. Konsep ini juga selaras dengan prinsip perlindungan martabat dalam hukum Indonesia, seperti yang tercantum dalam Pasal 1 UU PDP yang mengakui data pribadi sebagai bagian dari hak asasi manusia.[23]

Adapun langkah yang dapat dilakukan dalam pencegahan terhadap penyalahgunaan teknologi artificial intelligence (deepfake) ialah terhadap teknologi artificial intelligence (deepfake) hanya boleh digunanakan untuk wajah penggunanya sendiri dengan mekanisme menerapkan sistem verivikasi wajah atau biometrik atau face recognition technology. FRT bekerja dengan cara memindai wajah seseorang melalui bentuk mata, bibir, mulut, hidung, dan ukuran wajah secara mendetail. Cara bekerja teknologi ini adalah dengan mendeteksi, menganalisis, mengubah, serta mengidentifikasi. Awalnya, teknologi ini akan mendeteksi wajah seseorang. Kemudian, teknologi akan menganalisis struktur wajah orang tersebut agar mendapatkan ciri unik sehingga tidak ada kesamaan dengan orang lain. Analisis tersebut akan diubah kedalam bentuk face print yang akan digunakan sebagai kode numerik untuk membedakan wajah orang yang satu dengan lain. Setelah melalui tahap ini, maka sistem akan melakukan identifikasi. Identifikasi ini akan tersimpan di dalam basis data atau database. Dengan melakukan langkah verivikasi wajah atau biometrik atau face recognition technology terhadap pengguna platform deepfake membuat teknologi artificial intelligence (deepfake) tersebut tidak dapat disalahgunakan untuk membuat konten foto atau video palsu menggunakan wajah orang lain tanpa izin.

C. PENUTUP

Konsep pertanggungjawaban perdata terhadap penyalahgunaan teknologi artificial intelligence (deepfake) dapat disimpulkan bahwa dalam pertanggungjawaban hukum tetaplah memerlukan keterlibatan manusia, sehingga baik penyedia maupun pengguna platform deepfake dapat dimintai pertanggungjawaban atas kelalaian atau kesalahan yang menimbulkan kerugian,

[23] Raihani Latifatunnisa, *Urgensi Pembaruan Regulasi dalam Menanggulangi Penyalahgunaan Teknologi Artificial Intelligence dan Deepfake di Indonesia: Perspektif Perlindungan Hak Privasi*, Jurnal Hukum dan Kewarganegaraan, Vol.11, No.1 (2025), p.10.

hal demikian sebagaimana konsep perbuatan melawan hukum yang diatur dalam Pasal 1365 dan Pasal 1367 KUHPerdata. Kemudian implementasi pertanggungjawaban perdata atas penyalahgunaan deepfake masih menghadapi kompleksitas signifikan. Tantangan tersebut berasal dari aspek teknis, seperti keterbatasan generalisasi model deteksi dan tingginya realisme konten deepfake yang dipicu oleh teknologi deep learning serta aksesibilitas perangkat lunak yang mudah. Secara hukum, penegakan mengalami kendala dalam identifikasi pelaku, isu yurisdiksi lintas batas, dan kesulitan kuantifikasi kerugian imateriil. Selain itu, terdapat kekosongan hukum spesifik yang secara eksplisit mengatur deepfake, menjadikan UU yang ada bersifat umum dan belum adaptif terhadap karakteristik manipulasi berbasis AI. Oleh karena itu, diperlukan pendekatan holistik untuk menjawab tantangan ini. Solusi krusial mencakup reformasi regulasi melalui pembentukan norma lex specialis yang mengakomodasi kerugian digital baru dan menegaskan pertanggungjawaban strict liability platform digital dalam moderasi konten. Selanjutnya, peningkatan literasi hukum dan digital masyarakat menjadi esensial untuk memperkuat posisi korban. Terakhir, kerja sama internasional merupakan pilar utama dalam penegakan hukum siber lintas negara. Melalui sinergi pembaruan hukum nasional, penguatan peran aktor digital, dan kolaborasi global, diharapkan sistem hukum dapat secara efektif memberikan perlindungan hak asasi manusia, khususnya hak atas privasi dan kehormatan pribadi, di tengah perkembangan teknologi deepfake.

DAFTAR PUSTAKA

Buku

Djojodirdjo, M.A. Moegni. 1976. *Perbuatan Melawan Hukum*. Jakarta. Pradnya Paramita.

Fuady, Munir. 2018. *Perbuatan Melawan Hukum Pendekatan Kontemporer.* Bandung. Penerbit Citra Aditya Bakti.

Harahap, M. Yahya. 2016. *Hukum Perseroan Terbatas*. Jakarta. Sinar Grafika.

Kelsen, Hans (terj. Raisul Mutaqien). 2006. *Teori Hukum Murni*. Bandung. Nuansa & Nusa Media.

Kelsen. Hans (terj. Soemardi). 2007. *General Theory Of Law and State. Teori Umum Hukum dan Negara. Dasar-Dasar Ilmu Hukum Normatif sebagai Ilmu Hukum Deskriptif Empirik.* Jakarta: BEE Media Indonesia.

Marzuki, Peter Mahmud. 2016. *Penelitian Hukum, Edisi Revisi. Cetakan Ke-12*. Bandung. Pustaka Ramadhan.

Triwulan, Shinta Titik. 2010. *Perlindungan Hukum Bagi Pasien.* Jakarta: Prestasi Pustaka.

Publikasi

Coccomini, Andrea, Marco Bertini dan Alberto Del Bimbo. *Deepfake Detection: Challenges and Solutions*. Journal of Imaging. Vol.9. No.1 (2023).

Halipah, Gisni dkk.. *Tinjauan Yuridis Konsep Perbuatan Melawan Hukum dalam Konteks Hukum Perdata*. Jurnal Serambi Hukum. Vol.16. No.1 (2023).

Hapid, Fasa Muhamad dkk. *Penerapan Asas Geen Straf Zonder Schuld dalam Penindakan terhadap Kejahatan Penyalahgunaan Teknologi Deepfake*. Jurnal USM Law Review. Vol.7. No.3 (2024).

Jasmine, Alifia, Benny Djaja dan Maman Sudirman. *Tanggung Jawab Notaris dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jurnal Ilmu Hukum, Humaniora dan Politik. Vol.5. No.1 (November 2024).

Jufri, M. Ariq Abir dan Akbar Kurnia. *Aspek Hukum Internasional dalam Pemanfaatan Deepfake Technology terhadap Perlindungan Data Pribadi*. Uti Possidetis: Journal of International Law. Vol.2. No.1 (2021).

Kiliç, Büşra dan Mehmet Emin Kahraman. *Current Usage Areas of Deepfake Applications with Artificial Intelligence Technology*. İletişim ve Toplum Araştırmaları Dergisi. Vol.3. No.1 (2023).

Latifatunnisa, Raihani. *Urgensi Pembaruan Regulasi dalam Menanggulangi Penyalahgunaan Teknologi Artificial Intelligence dan Deepfake di Indonesia: Perspektif Perlindungan Hak Privasi*. Jurnal Hukum dan Kewarganegaraan. Vol.11. No.1 (2025).

Mayana, Ranti Fauza. *Legal Issues of Artifi cial Intelligence Generated Works: Challenges on Indonesian Copyright Law*. Law Reform. Vol.20. No.1 (2024).

Mutiara, Upik dan Romi Maulana. *Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi*. Indonesian Journal of Law and Policy Studies. Vol.1. No.1 (2020).

Nurmantani, Ni Nyoman Ari Diah dan Nyoman A. Martana. *Perlindungan Hukum terhadap Data Pribadi Peminjam dalam Layanan Aplikasi Pinjaman Online*. Journal Ilmu Hukum. Vol.1. No.1 (2019).

Panda, Jayanta Kumar dam Rajnandini Panigrahy. *Unmasking Deception In The Age Of Artificial Intelligence: A Comprehensive Analysis Of Indian Celebrity's Deepfakes News*. ShodhKosh: Journal of Visual and Performing Arts. Vol.4. No.2 (2023).

Putri, Silvia Mah Arani Iskandar dkk.. *Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum*. Jurnal Hukum Legalita. Vol.6. No.2 (2024).

Rachmadie, D. T. *Regulasi Penyimpangan Artificial Intelligence pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016*. Jurnal Hukum Pidana Dan Penanggulangan Kejahatan. Vol.9. No.2 (2016).

Singh, Hardeep dkk., *Deepfake as an Artificial Intelligence Tool for VFX Films*. 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) 2023.

Syahirah, Sabrina Nur. *Tinjauan Yuridis terhadap Penggunaan Teknologi Deepfake untuk Pornografi Melalui Artificial Intelligence (AI) di Indonesia*. Jurnal Inovasi Hukum dan Kebijakan. Vol.6. No.1 (2025).

Syaputra, Rendi. *Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake Melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia*. Respublica. Vol.24. No.01 (2024).

Verdoliva, L. *Media Forensics and DeepFakes: An Overview*. IEEE Journal of Selected Topics in Signal Processing. Vol.14. No.5 (2020).

Yuniarti, Siti. *Perlindungan Hukum Data Pribadi di Indonesia*. Jurnal BECOSS. Vol.1. No.1 (2019).

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.