Jurnal Ilmiah Hukum dan Hak Asasi Manusia (JIHHAM)
Vol 4, No 2, 2025, 73-82 https://doi.org/10.35912/jihham.v4i2.3937

Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP

(Legal Implications of Deepfake: A Review of the ITE Law and the PDP Law)

Rafi Satrya Arvitto
Universitas Negeri Surabaya, Jawa Timur, Indonesia
rafi.22085@mhs.unesa.ac.id

Riwayat Artikel
Diterima pada 31 Juli 2024
Revisi 1 pada 12 Agustus 2024
Revisi 2 pada 16 Oktober 2024
Revisi 3 pada 24 Oktober 2024
Disetujui pada 30 Oktober 2024

Abstract
Purpose: This study aims to analyze the regulation of deepfake technology usage within the legal framework of Indonesia, particularly concerning the Information and Electronic Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP). The main focus of this research is to identify whether existing regulations are sufficiently effective in addressing the threats posed by the misuse of deepfake technology and to assess the extent to which legal gaps affect the protection of victims.
Methodology: This research employs a normative juridical approach with a statute-based method. The data used in this study includes primary and secondary legal materials, including relevant regulations and literature discussing deepfake technology and its impact on the law.
Results: The research findings reveal that while UU ITE and UU PDP regulate data falsification and personal data protection in general, they do not specifically address the use of deepfake technology. This has resulted in a legal gap that causes uncertainty in handling deepfake cases in Indonesia. As a consequence, many abuses of this technology cannot be clearly addressed under existing regulations.
Limitations: This study is limited to an analysis of existing regulations in Indonesia and does not include a comparative study with regulations in other countries. Furthermore, the research does not cover technical solutions related to deepfake detection, which could be part of a preventive approach.
Contribution: This research contributes to understanding the shortcomings of regulations concerning deepfake technology in Indonesia and emphasizes the need for updates or additions to the legal framework to address these specific crimes. The study also provides a foundation for the development of more effective legal policies to tackle digital threats, particularly in relation to personal data protection and the misuse of AI technology.

Keywords: *Deepfake technology, Personal Data Protection Law (UU PDP), Information and Electronic Transactions Law (UU ITE), cybercrime, AI technology.*

How to cite: Arvitto, R, S. (2025). Implikasi Hukum Deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2), 73-82.

1. Pendahuluan

Perkembangan teknologi *artificial intelligence* atau bisa disingkat AI, mempermudah pekerjaan manusia sehari-hari. Contohnya yaitu ChatGPT, AI tersebut bisa menjawab segala pertanyaan kita hanya dengan hitungan detik. Program Pembangunan Perserikatan Bangsa-Bangsa (UNDP) juga

mendorong pemanfaatan AI untuk mempercepat pencapaian pembangunan berkelanjutan sekaligus terus menjaga dan memprioritaskan hak asasi manusia (Nwosu et al., 2024). Namun tidak semua perkembangan berbuah baik bagi masyarakat, salah satu contohnya yaitu *deepfake*. Teknologi *deepfake* adalah teknologi AI (*artificial intelligence*) yang dipakai untuk merubah bentuk suatu objek di dalam gambar atau video (Angelika Septi Rahayu & Santoso, 2023). Teknologi *deepfake* menggunakan berbagai algoritma canggih untuk menghasilkan konten palsu baik berupa video maupun gambar. Salah satu alat pendeteksi *deepfake* yang paling banyak digunakan adalah GAN (*Generative Adversarial Network*), yang digunakan untuk membuat produk palsu dalam bentuk gambar dan video. Saat ini, teknologi *deepfake* semakin populer karena kemudahan penggunaan dan harganya yang terjangkau (Mutmainnah et al., 2024). Dari sudut pandang positif, teknologi deepfake dipandang sebagai hiburan bagi masyarakat. Namun jika dilihat secara negatif, teknologi deepfake ini menyebabkan merebaknya tindakan asusila yang bermuatan SARA, peretasan data informasi (*hacking*), dan penyebaran berita bohong (*hoax*) (Mutmainnah et al., 2024).

Pada tahun 2018, dua peneliti Italia mengembangkan perangkat lunak bernama Deeptrace yang bertujuan untuk mendeteksi foto dan video deepfake. Lebih dari 14.000 video deepfake diunggah ke internet pada tahun 2019, 96 di antaranya merupakan konten pornografi yang dibintangi oleh perempuan (Somers, 2020). Di era modern, teknologi manipulasi wajah, konversi teks ke audio, dan pembuatan karya tiga dimensi bukanlah hal baru. Pada tahun 1997, Christoph Bregler, Michele Covell, dan Malcolm Slaney menerbitkan jurnal yang mengulas metode untuk menyinkronkan suara dengan gerakan mulut, yang dimanfaatkan dalam industri film (Song, 2019). Teknologi *deepfake* ini awalnya diperkenalkan oleh Ian Goodfellow pada tahun 2014 dengan tujuan untuk hiburan semata. Salah satu penerapan awal dari teknologi *deepfake* adalah aplikasi Face Swap, yang memungkinkan pengguna untuk menukar wajah mereka dengan wajah orang lain dalam sebuah foto (Gandrova & Banke, 2023). Amerika Serikat telah mengambil langkah hukum melalui National Defense Authorization Act (NDAA), yang mewajibkan Direktur Intelijen Nasional untuk melaporkan penggunaan teknologi *deepfake* oleh pemerintah asing. Meski demikian, kebijakan ini dianggap belum sepenuhnya memadai dalam menghadapi tantangan yang ditimbulkan oleh *deepfake*, mengingat kemajuan teknologi yang terus berkembang pesat dan sering kali melampaui jangkauan regulasi. Hingga saat ini, hanya lima negara bagian di Amerika Serikat yang telah mengesahkan undang-undang terkait teknologi *deepfake*. Sejak 2019, negara bagian seperti Texas dan California telah melarang penggunaan *deepfake* untuk memengaruhi proses pemilu di masa depan (Gandrova & Banke, 2023).

2. Tinjuauan Pustaka

Penyalahgunaan aplikasi deepfake memiliki kaitan erat dengan kejahatan dunia maya (*cybercrime*), karena hasil manipulasi foto atau video deepfake umumnya disebarluaskan melalui media sosial yang bergantung pada jaringan internet. Oleh sebab itu, tindakan ini dapat dikategorikan sebagai bagian dari *cybercrime*. Dengan demikian, tindak pidana terkait penyalahgunaan *deepfake* perlu dianalisis berdasarkan undang-undang yang mengatur kejahatan siber, serta undang-undang yang mengatur dampak yang ditimbulkan dari penyalahgunaan teknologi tersebut. Dengan berkaitannya teknologi *deepfake* dengan kejahatan siber, pelaku penyebar *deepfake* akan pasti menutupi jejaknya di dunia maya. Jaringan pribadi virtual (VPN) dirancang untuk menyembunyikan identitas alamat IP pengguna, sehingga dapat memudahkan penjahat untuk melakukan aktivitas kriminal. Seperti kata pepatah, "tidak ada kejahatan yang sempurna" karena kejahatan tradisional selalu meninggalkan bekas. Namun saat ini, akses internet yang mudah memungkinkan terjadinya kejahatan dunia maya tanpa meninggalkan jejak dan tanpa saksi. Oleh karena itu, lembaga penegak hukum tidak hanya perlu meningkatkan kemampuan mereka dalam mendeteksi deepfake, namun juga berinvestasi pada kemampuan mereka untuk mengatasi tantangan teknologi yang terus berkembang (Europol, 2022). Pesatnya perkembangan teknologi *deepfake* menimbulkan pertanyaan tentang keberadaan regulasi yang relevan, khususnya di Indonesia. Sebagai teknologi yang memiliki manfaat sekaligus risiko, pengaturan hukum menjadi penting untuk mencegah penyalahgunaannya. Di Indonesia, perlindungan terhadap dampak negatif dari teknologi *deepfake* ini perlu ditinjau lebih jauh, terutama melalui kerangka Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Ketiadaan regulasi khusus yang mengatur penggunaan deepfake berbasis kecerdasan buatan (AI) di

Indonesia memunculkan keraguan di kalangan tertentu mengenai efektivitas sanksi yang dapat dijatuhkan kepada pelaku (Utama et al., 2023). Meskipun sudah ada UU ITE, UU Pornografi, dan UU Perlindungan Data Pribadi, ketiadaan aturan yang secara jelas mengatur penggunaan AI dan segala hal terkait *deepfake* akan mengurangi efektivitas perlindungan hukum bagi korban dari tindakan tersebut. Hingga saat ini, Indonesia belum memiliki peraturan yang secara khusus mengatur pembatasan penggunaan AI, termasuk terkait dengan teknologi *deepfake*. Berdasarkan penelitian yang dilakukan oleh Noerman dan Ibrahim, disimpulkan bahwa UU PDP dan UU ITE hanya mengatur pemalsuan data pribadi secara umum. Hal ini menyebabkan adanya kekosongan hukum, karena belum ada aturan yang mengatur tindak pidana *deepfake*. Kekosongan hukum ini menimbulkan ketidakpastian dalam penanganan tindak pidana *deepfake*, yang pada akhirnya dapat menimbulkan kebingungan di masyarakat, karena tidak ada pedoman yang jelas untuk membedakan informasi yang benar dan hoaks (No et al., 2024). Maka dari itu, penelitian ini berfokus untuk mencari tahu apakah *deepfake* sudah diatur secara spesifik di dalam UU ITE dan juga di dalam UU PDP.

3. Metodologi penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian yuridis normatif dengan jenis penelitian kualitatif, yakni dimana hukum dikonsepkan sebagai apa yang tertulis dalam peraturan perundang-undangan (*law in books*) atau hukum dikonsepkan sebagai kaidah atau norma yang merupakan patokan berperilaku manusia dianggap pantas. Penelitian hukum normatif ini didasarkan pada bahan hukum primer dan bahan hukum sekunder yaitu penelitian yang mengacu pada norma-norma yang terdapat dalam peraturan perundang-undangan. Sehubungan dengan jenis penelitian yuridis normatif maka pendekatan yang digunakandalam tulisan ini adalah pendekatan perundang-undangan (*statute approach*).

4. Hasil dan pembahasan

4.1 Pengaturan Deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

4.1.1 Definisi Deepfake dalam Konteks Hukum

Deepfake adalah teknologi berbasis kecerdasan buatan (AI) yang umum digunakan untuk memalsukan atau memanipulasi foto, video, dan audio dengan menggunakan teknik pemindaian mendalam pada gambar orang menggunakan teknologi *Deep Learning* (Amelia et al., 2024). *Deepfake* merujuk pada video yang menyisipkan wajah realistis pada tubuh individu lain, bertujuan menciptakan video baru dengan representasi yang tidak sebenarnya (Spivak, 2019). Penjelasan lain mengungkapkan bahwa istilah *deepfake* berasal dari gabungan dua kata, yaitu "*deep learning*" dan "*fake*." *Deepfake* mengacu pada audio-visual dengan tingkat realisme tinggi yang dihasilkan menggunakan teknologi *deep learning* (Noval, 2019) Ada beberapa jenis video deepfake yang bisa dikenali saat ini. Salah satunya adalah video asli yang diubah dengan cara "mengganti" wajah orang dalam video dengan wajah orang lain, sehingga terlihat seolah-olah orang baru tersebut benar-benar melakukan apa yang ada di video. *Deepfake* kerap dimanfaatkan untuk menggantikan wajah seseorang dengan wajah orang lain, baik dalam bentuk video, gambar, maupun audio. Salah satu contoh paling umum adalah pornografi *deepfake*. Porno *deepfake* menggunakan teknologi AI untuk menggantikan wajah seseorang untuk membuat konten pornografi palsu. Hasilnya adalah kualitas visual yang sangat realistis seperti aslinya (Syaputra, 2024). Masalah ini membawa banyak dampak buruk bagi korban, terutama ketika foto atau video mereka digunakan untuk tujuan yang merugikan. Korban bisa mengalami tekanan psikologis, kehilangan nama baik di masyarakat, serta merasa privasinya dilanggar dan keamanannya terancam. Selain digunakan untuk pornografi *deepfake*, teknologi *Deepfake* juga dimanfaatkan dalam berbagai modus lainnya. Contohnya, membuat video, gambar, atau suara palsu untuk mengajukan pinjaman online, atau memalsukan suara seseorang agar terdengar seperti pejabat, yang kemudian dipakai pelaku untuk kepentingan pribadi. Deepfake dapat dikategorikan sebagai bentuk Kekerasan Gender Berbasis Online (KGBO). Perbuatan ini berpotensi menimbulkan berbagai dampak negatif bagi korban, antara lain (Kusuma & Arum, 2019):

a) Dampak psikologis
   Korban dapat mengalami trauma atau gangguan stres pascatrauma (PTSD).
b) Dampak sosial
   Terasing dari lingkungan, kehilangan rasa percaya diri, dan menjadi sasaran penghinaan.
c) Dampak ekonomi
   Mengalami kerugian finansial, reputasi yang rusak, hingga kehilangan sumber penghasilan.

d) Dampak pada mobilitas
   Kehilangan kebebasan bergerak, baik dalam ruang online maupun offline.
e) Dampak pada ekspresi diri
   Menutup diri dan kehilangan rasa percaya terhadap teknologi digital.

Teknologi deepfake memungkinkan orang untuk membuat propaganda dengan menggunakan gambar tokoh publik, yang bisa sangat berbahaya, terutama di negara yang sedang menghadapi konflik antargolongan. Propaganda semacam ini bisa memicu gerakan massa yang berpotensi menimbulkan ketegangan atau konflik fisik. Seiring berjalannya waktu, kualitas video deepfake akan semakin tinggi, sehingga sulit untuk membedakan mana yang asli dan mana yang palsu. Hal ini membuat penyebaran video berisi propaganda menjadi lebih mudah, apalagi jika tokoh yang ditampilkan memiliki banyak pengikut (Khusna & Pangestuti, 2019). Banyak orang yang menjadikan DeepFake sebagai sumber penghasilan tambahan, bahkan utama, karena proses pembuatannya yang relatif mudah. Namun, kemudahan ini sering disalahgunakan untuk mengedit gambar atau video seseorang menjadi tidak pantas atau merugikan. Jika diketahui, para pelaku bisa dikenakan tindakan hukum (Tambun et al., 2024).

4.1.2 Relevansi Deepfake dengan UU ITE

Relevansi teknologi *deepfake* dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) semakin penting untuk dibahas, mengingat potensi penyalahgunaan yang dapat merugikan individu maupun masyarakat luas, baik dalam konteks pencemaran nama baik, penyebaran informasi palsu, maupun pelanggaran privasi melalui media digital. Salah satu tantangan utama yang muncul dari transformasi digital adalah terkait privasi. Saat ini, manusia semakin sering berbagi informasi dan data yang menjadi elemen penting dalam konektivitas big data, seperti proses pencarian, pengumpulan, investigasi, hingga analisis perilaku. Akibatnya, perlindungan hak privasi yang sebelumnya hanya berlaku di dunia nyata kini meluas ke dunia virtual dan digital (Yunanda et al., 2024). Undang-Undang ITE, yang mulai berlaku pada April 2008, memberikan terobosan penting dengan mengatur dunia maya di Indonesia. Dikenal sebagai *Cyber Law*, undang-undang ini berlaku tidak hanya bagi warga negara Indonesia, tetapi juga bagi orang di luar negeri yang perbuatannya dapat menimbulkan akibat hukum di Indonesia atau merugikan kepentingan Indonesia. *Cybercrime* dapat didefinisikan secara luas sebagai "tindakan melanggar hukum di mana komputer digunakan sebagai alat, target, atau keduanya." Dalam konteks *Cybercrime*, *cybercriminal* adalah seseorang yang melakukan tindakan ilegal dengan niat untuk melakukan kejahatan (Dokku & Kandula, 2021).

Saat bekerja keras untuk menciptakan kenyamanan dan kesenangan di dunia berteknologi tinggi, orang-orang lupa tentang efek samping yang bisa menyertai. Celah inilah yang dimanfaatkan oleh penjahat siber untuk mengendalikan setiap gerakan manusia (Roy, 2022). Undang-Undang ITE juga berfungsi sebagai payung hukum untuk transaksi dan perdagangan elektronik di dunia maya (*cyberspace*). Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diberlakukan pada April 2008, telah menjadi terobosan hukum di Indonesia dengan memberikan dasar hukum pertama kali untuk dunia maya. Namun, banyak permasalahan muncul, terutama terkait pasal-pasal tentang pencemaran nama baik atau delik reputasi, yang dianggap memiliki cacat bawaan dan inkonsistensi dalam penerapannya (Setiawan, 2021). UU ITE mencakup sekitar 11 pasal yang mengatur berbagai perbuatan yang dilarang, dengan total hampir 22 jenis tindakan yang tidak diperbolehkan (Raharja, 2019). Dari pasal-pasal tersebut, terdapat 3 pasal yang berpotensi membahayakan pengguna media elektronik. Pasal-pasal ini mengatur larangan-larangan tertentu di dunia maya yang bisa dilanggar tanpa disadari oleh penggunanya. Pasal-pasal tersebut antara lain Pasal 27 ayat (1) dan (3), Pasal 28 ayat (2), serta Pasal 45 ayat (1) dan (2). Sebuah artikel berita nasional menyebutkan bahwa ujaran kebencian adalah salah satu bentuk kejahatan dunia maya yang paling sering terjadi di Indonesia. Kasus ini banyak terjadi melalui media sosial dan platform lainnya.

Pada tahun 2017, Polri mencatat 3.325 kasus ujaran kebencian, sementara di tahun 2016 jumlahnya mencapai 1.829 kasus. Sayangnya, meskipun ada banyak kasus *cybercrime* lainnya, perhatian dari pemerintah terhadap masalah ini masih terbilang minim (Ramadhani, 2023). Saat ini, jumlah pengguna

ponsel aktif di Indonesia, termasuk kartu SIM-nya, telah mencapai 281,9 juta. Hal ini memungkinkan masyarakat untuk berbagi informasi dengan sangat cepat. Media sosial dan aplikasi pesan instan menjadi platform pilihan utama bagi pengguna (Mufid & Hariandja, 2019). Dengan banyaknya pengguna ponsel beserta media sosial, sudah jelas pasti ada konsekuensi yang mengikuti, yaitu maraknya kasus *cybercrime* yang sering terjadi. Dengan UU ITE yang implementasinya lebih sering berfokus kepada kasus *cybercrime* berupa *bullying*, pemerintah masih kurang memperhatikan relevansi *deepfake* dengan UU ITE. UU ITE memiliki sejumlah pasal yang dapat digunakan untuk menangani penyalahgunaan teknologi *deepfake*, meskipun belum secara spesifik mengatur tentang teknologi ini. Salah satu pasal yang relevan adalah Pasal 27 ayat (1), yang melarang distribusi konten yang melanggar kesusilaan. Deepfake yang digunakan untuk membuat konten tidak senonoh, seperti pornografi atau pelecehan seksual, dapat dijerat dengan pasal ini. Pasal 27 ayat (3), yang melarang pencemaran nama baik, juga relevan jika *deepfake* digunakan untuk merusak reputasi seseorang, misalnya dengan mengaitkan individu dengan tindakan atau situasi yang tidak sesuai kenyataan. Selanjutnya, Pasal 28 ayat (1) melarang penyebaran berita bohong atau informasi palsu yang dapat merugikan konsumen di bidang elektronik. Jika *deepfake* digunakan untuk menyebarkan hoaks atau manipulasi informasi yang dapat merugikan masyarakat atau individu tertentu, pasal ini dapat diterapkan. Pasal 28 ayat (2), yang mengatur tentang larangan menyebarkan konten yang memicu kebencian atau permusuhan berbasis SARA, juga dapat digunakan jika *deepfake* dipakai untuk tujuan provokasi atau menyulut konflik. Pasal 29 melarang pengiriman informasi elektronik yang mengandung ancaman kekerasan atau tindakan menakut-nakuti. Jika *deepfake* dimanfaatkan untuk membuat ancaman atau intimidasi terhadap seseorang, maka tindakan ini juga bisa dijerat hukum. Selain itu, Pasal 36 menyatakan bahwa perbuatan yang menyebabkan kerugian kepada orang lain dapat dikenakan sanksi hukum, yang relevan jika penggunaan *deepfake* merugikan korban secara finansial, sosial, atau emosional. Namun, meskipun beberapa pasal dalam UU ITE dapat digunakan untuk mengatur penyalahgunaan *deepfake*, undang-undang ini belum secara spesifik membahas teknologi tersebut. Hal ini bisa menjadi kendala karena penerapan hukum masih bergantung pada interpretasi masing-masing pasal. Selain itu, perkembangan teknologi *deepfake* yang semakin canggih membuat deteksi dan pembuktian pelanggaran menjadi tantangan tersendiri. Oleh karena itu, diperlukan regulasi yang lebih spesifik dan komprehensif untuk mengatur penyalahgunaan *deepfake*, sehingga dapat melindungi masyarakat dari dampak negatif yang ditimbulkannya.

4.1.3 Tantangan dalam Pengaturan Deepfake di UU ITE

Kelemahan regulasi UU ITE dalam menangani penyalahgunaan teknologi deepfake terletak pada ketiadaan pengaturan yang spesifik dan eksplisit mengenai teknologi ini, sehingga menimbulkan berbagai hambatan dalam penegakan hukum. Tanpa definisi yang jelas tentang deepfake, pasal-pasal yang ada harus diinterpretasikan untuk mencakup kejahatan ini, yang sering kali menyebabkan ketidakpastian hukum. Perkembangan teknologi deepfake yang pesat, dengan kemampuan menghasilkan konten yang semakin sulit dibedakan dari aslinya, juga memperparah situasi karena menyulitkan proses identifikasi dan pembuktian di pengadilan.

Selain itu, UU ITE cenderung lebih berorientasi pada perbuatan umum di dunia maya tanpa memberikan perhatian khusus pada teknologi baru seperti deepfake, sehingga kurang memadai untuk pencegahan maupun penanganan secara efektif. Dampaknya, korban dari penyalahgunaan deepfake, seperti kasus pencemaran nama baik, penyebaran hoaks, atau pelecehan digital, tidak selalu mendapatkan perlindungan hukum yang optimal. Ketiadaan pengaturan ini juga menghambat upaya edukasi publik mengenai dampak hukum penggunaan deepfake, yang berpotensi dimanfaatkan oleh pelaku untuk menjalankan aksinya tanpa rasa takut terhadap konsekuensi hukum. Oleh karena itu, diperlukan revisi atau penambahan dalam UU ITE untuk mengakomodasi perkembangan teknologi ini secara spesifik, sehingga mampu memberikan landasan hukum yang lebih kuat untuk penegakan hukum dan perlindungan bagi masyarakat.

Regulasi yang ada saat ini lebih berfokus pada peran AI sebagai agen elektronik, yaitu perangkat yang dirancang untuk secara otomatis melakukan tindakan berdasarkan informasi elektronik. Namun, aturan tersebut belum sepenuhnya menyentuh isu yang lebih kompleks, seperti etika, privasi, dan dampak sosial dari penggunaan teknologi AI. Ketidakjelasan dalam kerangka hukum juga menyebabkan

kurangnya kejelasan mengenai tanggung jawab dalam pemanfaatan AI. Selain itu, ketentuan yang ada lebih menitikberatkan pada larangan mentransmisikan, mendistribusikan, atau menyediakan akses terhadap Informasi Elektronik atau Dokumen Elektronik yang mengandung unsur melanggar kesusilaan, daripada langsung mengatur tindakan terkait pelanggaran kesusilaan itu sendiri (Amelia et al., 2024). Jika norma atau tindak pidana yang dikenakan kepada pelaku kejahatan *deepfake* online, yang melibatkan teknologi kecerdasan buatan, tidak dijelaskan dengan jelas dalam hukum pidana Indonesia, terdakwa bisa membela diri dan terbebas dari tuntutan (*ontslag van rechtsvervolging*). Ini terjadi karena perbuatan yang dilakukan tidak dijelaskan secara spesifik dalam hukum pidana Indonesia, atau karena kejahatan tersebut menggunakan teknologi canggih yang belum diatur dalam peraturan yang ada (Putra, 2023).

4.2 Pengaturan Deepfake dalam Undang-Undang Perlindungan Data Pribadi (UU PDP)

4.2.1 Deepfake dalam Perspektif Perlindungan Data Pribadi

Deepfake, sebagai salah satu teknologi berbasis kecerdasan buatan, telah berkembang pesat dan memunculkan berbagai tantangan hukum, terutama dalam hal perlindungan data pribadi. Dalam perspektif Undang-Undang Perlindungan Data Pribadi (UU PDP), penyalahgunaan teknologi ini dapat berpotensi melanggar hak individu atas data pribadi mereka, seperti wajah atau suara yang digunakan tanpa izin. Penggunaan *deepfake* untuk tujuan manipulasi atau pencemaran nama baik dapat menimbulkan dampak serius terhadap privasi dan reputasi seseorang. Oleh karena itu, penting untuk mengkaji sejauh mana UU PDP dapat memberikan perlindungan terhadap penyalahgunaan teknologi ini dan bagaimana penerapan regulasi yang ada dapat menjaga hak-hak individu di era digital yang semakin canggih. Seiring dengan kemajuan teknologi, kebutuhan akan data dan informasi pun semakin meningkat. Untuk melindungi korban dari penyalahgunaan data pribadi melalui teknologi *deepfake*, langkah pertama yang perlu dilakukan adalah meningkatkan kesadaran masyarakat, khususnya aparat penegak hukum, tentang adanya penyalahgunaan *deepfake* sebagai bentuk kekerasan berbasis online (Oktallia & Ariana, 2022).

Di beberapa negara Eropa, telah diterapkan perlindungan data pribadi yang sangat baik untuk menjaga keamanan informasi pribadi warganya. Di mana warga negara memiliki hak untuk menuntut pemenuhan apa yang dikenal dengan "hak untuk dilupakan" (RTBF) (Noval, 2019). Dampak negatif yang ditimbulkan oleh teknologi *deepfake* menimbulkan kekhawatiran di kalangan masyarakat, terutama karena kemampuannya dalam memanipulasi wajah manusia. Saat ini, deepfake dapat menghasilkan gambar wajah yang sangat mirip dengan aslinya, sehingga sulit untuk dibedakan. Oleh karena itu, sangat penting untuk mengembangkan sebuah sistem yang dapat membedakan wajah asli dari yang dibuat oleh *deepfake*. Pengembangan sistem ini diharapkan dapat mengurangi kekhawatiran masyarakat dengan memudahkan identifikasi wajah yang sebenarnya. Salah satu metode yang sering digunakan untuk tujuan ini adalah *Convolutional Neural Network* (CNN) (Marcella et al., 2022). Berbagai penelitian telah dilakukan untuk mengklasifikasikan wajah manusia menggunakan metode Convolutional Neural Network (CNN), yang menunjukkan hasil yang signifikan. Sebagai contoh, penelitian yang mengklasifikasikan jenis kulit wajah berhasil mencapai akurasi 100% pada tahap pelatihan, 88% pada pengujian, dan 90% pada pengujian dengan data baru. Penelitian lain yang mengklasifikasikan wajah bermasker menunjukkan akurasi sebesar 99,20% pada data pelatihan dan 70,59% pada data validasi dengan 3 layer, sedangkan dengan 5 layer, akurasi pelatihan mencapai 98,20% dan akurasi validasi sebesar 82,35%. Selain itu, penelitian terkait sistem pengenalan wajah memperoleh akurasi 99,84%. Penelitian untuk klasifikasi wajah pada gambar bergerak menunjukkan akurasi 90% pada pelatihan dan 95% pada validasi. Terakhir, penelitian yang mengklasifikasikan jenis kulit wajah mencapai akurasi 99,51%. Hasil-hasil ini mengindikasikan bahwa metode CNN sangat efektif dan akurat dalam melakukan klasifikasi terhadap citra dan gambar (Mu et al., 2024). Dengan penjelasan sebelum-sebelumnya, bisa dikatakan bahwa hubungan antara teknologi *deepfake* dengan UU PDP saling melengkapi. Dengan seringnya masyarakat berinteraksi satu sama lain dan bertukar informasi, bisa saja informasi tersebut diambil oleh pihak yang tidak bertanggung jawab dan dijadikan *deepfake* untuk kepentingan pribadi.

4.2.2 Analisis Pengaturan dalam UU PDP

Dengan kemajuan zaman dan teknologi yang semakin pesat, kejahatan siber (*cybercrime*) juga ikut berkembang, menghasilkan berbagai bentuk kejahatan baru dengan metode yang lebih canggih. Di era digital saat ini, masalah kebocoran data menjadi semakin mendesak. Keamanan data pribadi menjadi perhatian utama karena data ini dapat disalahgunakan untuk berbagai kejahatan seperti pencurian identitas, penipuan, dan aktivitas ilegal lainnya (Sahatatua et al., 2024). Kejahatan siber kini tidak hanya mencakup hal-hal seperti *hacking*, *cracking*, atau *carding*, tetapi juga beragam jenis kejahatan lainnya yang lebih spesifik, seperti *probe* (usaha untuk mengakses sistem), *scan* (probe dalam jumlah besar), *account compromise* (penggunaan akun secara ilegal), *root compromise* (akses akun dengan hak penuh), *denial of service* (DoS) yang membuat jaringan tidak bisa digunakan, penyalahgunaan nama domain, dan masih banyak lainnya (Ekawati, 2018). Pelaku kejahatan siber sering kali mengeksploitasi data pribadi korban melalui teknik phishing, yaitu suatu tindakan untuk mendapatkan informasi pribadi yang bersifat rahasia dengan cara menipu korban (Wibowo & Fatimah, 2017). Phishing adalah usaha untuk mendapatkan informasi pribadi seseorang dengan cara menipu. Data yang biasanya menjadi target phishing antara lain informasi pribadi seperti nama, usia, dan alamat, data akun seperti username dan password, serta informasi finansial seperti nomor kartu kredit dan rekening bank (Sutarli & Kurniawan, 2023).

Bocornya data pribadi dapat menyebabkan berbagai masalah, seperti spam melalui email dan SMS, serta kejahatan siber lainnya yang bisa merugikan masyarakat. Oleh karena itu, melindungi data pribadi sangat penting di era digital saat ini (Sutarli & Kurniawan, 2023). Dengan semakin canggihnya teknologi, termasuk dalam pembuatan deepfake, ancaman terhadap privasi dan data pribadi menjadi semakin besar. Deepfake, yang memungkinkan pembuatan konten media yang sangat realistis namun palsu, dapat digunakan untuk memanipulasi gambar, video, atau suara seseorang tanpa izin. Hal ini dapat menimbulkan berbagai dampak negatif, mulai dari penyalahgunaan identitas, pencemaran nama baik, hingga kerugian finansial dan reputasi bagi korban. Oleh karena itu, perlindungan terhadap data pribadi menjadi sangat penting, dan peraturan yang ada harus mampu mengakomodasi ancaman baru yang ditimbulkan oleh teknologi ini. Dalam hal ini, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru-baru ini diundangkan di Indonesia dapat berperan penting. UU ini mengatur tentang perlindungan data pribadi warga negara, termasuk dalam hal pengumpulan, pengolahan, penyimpanan, dan penyebaran data pribadi. Deepfake yang menyalahgunakan data pribadi untuk menciptakan konten palsu dapat dikategorikan sebagai pelanggaran terhadap perlindungan data pribadi, karena melibatkan penggunaan data seseorang tanpa izin yang jelas.

Undang-Undang Perlindungan Data Pribadi (UU PDP) merupakan regulasi yang penting dalam memberikan perlindungan terhadap data pribadi individu di Indonesia, terutama di era digital yang semakin berkembang pesat. Meskipun UU PDP tidak secara eksplisit mengatur tentang fenomena *deepfake*, namun pengaturan dalam UU ini dapat diterapkan untuk menangani penyalahgunaan data pribadi yang digunakan untuk pembuatan *deepfake*. UU PDP memberikan landasan hukum untuk melindungi data pribadi individu dari penyalahgunaan, yang menjadi relevansi utama dalam konteks deepfake. Pasal 4 dalam UU PDP menyebutkan bahwa setiap orang memiliki hak untuk memperoleh perlindungan data pribadi yang digunakan oleh pihak lain, yang berarti data pribadi yang diambil untuk tujuan apapun, termasuk untuk pembuatan *deepfake*, harus dilakukan dengan izin dari subjek data tersebut. Dalam hal ini, *deepfake* yang memanipulasi citra atau suara seseorang tanpa izin jelas merupakan pelanggaran terhadap hak individu untuk mengontrol data pribadinya. Teknologi *deepfake* sering memanfaatkan gambar, suara, dan informasi pribadi tanpa sepengetahuan atau persetujuan individu yang bersangkutan, yang melanggar ketentuan Pasal 4 tersebut. Lebih lanjut, Pasal 9 UU PDP menekankan bahwa pengumpulan dan pengolahan data pribadi hanya boleh dilakukan dengan persetujuan dari subjek data.

Jika data pribadi digunakan untuk membuat deepfake tanpa izin, maka hal ini jelas melanggar pasal ini. Misalnya, jika seseorang menggunakan gambar atau video orang lain untuk membuat konten deepfake yang merugikan, maka mereka telah melanggar hak atas data pribadi yang diatur dalam UU PDP. Pasal ini juga mengatur bahwa subjek data berhak untuk menarik persetujuan mereka kapan saja, yang berarti penggunaan data pribadi untuk deepfake yang sudah ada tanpa persetujuan yang sah harus dihentikan.

Pasal 12 UU PDP mengatur hak individu untuk mengakses data pribadi mereka yang disimpan oleh pihak pengendali data, sementara Pasal 15 memberikan hak kepada individu untuk mengajukan permintaan penghapusan data pribadi mereka. Dalam konteks deepfake, hal ini sangat relevan jika seseorang merasa bahwa data pribadinya telah disalahgunakan untuk membuat konten palsu yang merugikan. Individu yang menjadi korban deepfake berhak untuk meminta agar data pribadi yang digunakan dalam konten tersebut dihapus dan tidak lagi digunakan untuk tujuan lebih lanjut. Ini memberikan individu kontrol lebih besar atas penggunaan data pribadinya di dunia digital. Selain itu, Pasal 21 UU PDP memberikan kewajiban kepada pihak pengendali data untuk memastikan bahwa data pribadi yang mereka kumpulkan dan olah aman dari potensi kebocoran atau penyalahgunaan. Deepfake yang mengandalkan data pribadi, seperti foto atau video seseorang, memerlukan perlindungan ekstra agar tidak jatuh ke tangan yang salah. Penyalahgunaan data pribadi yang digunakan untuk deepfake tanpa pengawasan yang ketat dapat menciptakan risiko besar terhadap privasi dan keamanan seseorang. Oleh karena itu, pihak pengendali data wajib menjaga data pribadi dengan sangat hati-hati agar tidak digunakan secara tidak sah dalam pembuatan deepfake. Namun, meskipun UU PDP memberikan dasar yang kuat untuk melindungi data pribadi dalam konteks teknologi baru seperti deepfake, masih ada ruang untuk pengembangan lebih lanjut. Misalnya, belum ada ketentuan yang secara eksplisit mengatur fenomena deepfake dalam UU PDP. Oleh karena itu, diperlukan revisi atau tambahan pasal-pasal yang secara spesifik mengatur penyalahgunaan data pribadi untuk pembuatan deepfake, dengan memperjelas sanksi dan tanggung jawab hukum bagi para pelaku. Dengan demikian, meskipun UU PDP tidak secara langsung mencakup masalah deepfake, pengaturan yang ada dalam UU ini dapat diterapkan untuk melindungi individu dari penyalahgunaan data pribadi yang digunakan dalam pembuatan konten deepfake. Regulasi ini menjadi penting untuk menjamin perlindungan data pribadi di era digital, di mana teknologi terus berkembang dan menghadirkan ancaman baru terhadap privasi individu.

4.2.2 Hambatan dan Peluang dalam Mengatur Deepfake melalui UU PDP

Mengatur fenomena *deepfake* melalui Undang-Undang Perlindungan Data Pribadi (UU PDP) menghadirkan beberapa hambatan dan peluang. Salah satu hambatan utama adalah kenyataan bahwa UU PDP tidak secara spesifik mengatur teknologi baru seperti *deepfake*. Meskipun UU ini memberikan perlindungan terhadap data pribadi, aplikasi praktis dari regulasi ini dalam menghadapi ancaman deepfake masih terbatas. Misalnya, definisi dan ruang lingkup penyalahgunaan data pribadi dalam pembuatan deepfake belum diatur secara rinci, sehingga membuat penerapan hukum menjadi kurang jelas. Selain itu, teknologi *deepfake* yang terus berkembang memerlukan pendekatan hukum yang lebih fleksibel dan dinamis, yang mungkin belum sepenuhnya tercakup dalam kerangka hukum yang ada. Namun, ada peluang besar dalam menggunakan UU PDP untuk melindungi individu dari penyalahgunaan data pribadi dalam pembuatan deepfake. UU PDP memberikan dasar hukum yang kuat terkait hak individu atas perlindungan data pribadi, termasuk hak untuk memberi persetujuan atau menolak penggunaan data pribadinya. Hal ini bisa menjadi landasan untuk mengembangkan regulasi yang lebih tegas dalam konteks *deepfake*, seperti mewajibkan persetujuan eksplisit untuk penggunaan data pribadi dalam pembuatan konten media.

Selain itu, perkembangan teknologi pengenalan wajah dan alat deteksi *deepfake* yang semakin canggih dapat menjadi peluang untuk memperkuat penerapan UU PDP dalam mengidentifikasi dan mencegah penyalahgunaan data pribadi. Dengan revisi atau penambahan pasal yang lebih spesifik tentang *deepfake*, UU PDP dapat menjadi alat yang efektif untuk menghadapi tantangan baru dalam perlindungan data pribadi di era digital. Mengatur ancaman dari teknologi deepfake melalui Undang-Undang Perlindungan Data Pribadi (UU PDP) memang menghadirkan tantangan besar, terutama terkait dengan perlindungan data pribadi yang digunakan untuk membuat konten palsu. Salah satu hambatan utamanya adalah kurangnya kejelasan dalam regulasi mengenai bagaimana data pribadi, seperti wajah atau suara, dapat dilindungi dari penyalahgunaan dalam pembuatan deepfake. Untuk mengatasi masalah ini, ada beberapa langkah yang bisa diambil. Pertama, perlu ada penjelasan lebih lanjut dalam UU PDP tentang bagaimana data pribadi bisa digunakan dalam pembuatan konten deepfake, serta persetujuan eksplisit yang harus didapatkan dari individu sebelum data mereka digunakan. Selain itu, pengembangan teknologi deteksi deepfake yang lebih canggih dan mudah diakses juga sangat penting untuk membantu mengidentifikasi konten palsu dengan cepat. Terakhir, penegakan hukum yang lebih

tegas dengan sanksi yang jelas bagi pelaku penyalahgunaan data pribadi dalam pembuatan deepfake juga diperlukan agar masyarakat merasa lebih aman.

5. Kesimpulan

Dalam penelitian ini, telah dibahas secara mendalam mengenai implikasi hukum dari teknologi deepfake, khususnya dalam konteks regulasi yang ada di Indonesia, yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Teknologi *deepfake*, yang memungkinkan pembuatan konten palsu dengan memanipulasi gambar dan suara, telah menimbulkan berbagai tantangan hukum yang mendalam, terutama dalam hal perlindungan data pribadi dan keamanan informasi. Penelitian ini sudah mencapai resolusi bahwa teknologi *deepfake* masih belum secara spesifik diatur didalam UU ITE dan UU PDP. Dengan tidak diaturnya *deepfake*, ada kemungkinan multitafsir dengan pasal-pasal tertentu di UU ITE dan UU PDP yang berkaitan dengan penyalahgunaan *deepfake*. Hal ini bisa dibuktikan di berbagai pasal di UU ITE yang hanya mengatur konsekuensi jika telah terjadinya perbuatan dengan itikad tidak baik yang melibatkan penggunaan teknologi, namun tidak mengatur penggunaan teknologi *deepfake* untuk melarang penggunaan *deepfake* yang ditujukan untuk kejahatan. Mengingat bahwa teknologi *deepfake* akan berkembang lebih pesat, maka urgensi untuk membuat rancangan Undang-Undang mengenai *deepfake* sangat diperlukan.

Limitasi dan studi lanjutan

Penelitian ini memiliki limitasi hanya untuk mengetahui apakah teknologi *deepfake* sudah diatur secara spesifik di UU ITE dan UU PDP. Dengan penjabaran yang sudah dilakukan, UU ITE dan UU PDP hanya mengatur secara umum. Untuk memperluas cakupan dari penelitian ini, bisa dilakukan dengan membawa urgensi konstruksi hukum mengenai pengaturan *deepfake* untuk menghindari multitafsir oleh para pengacara saat bertemu dengan kasus yang melibatkan teknologi *deepfake*.

Referensi

Amelia, Y. F., Kaimuddin, A., & Ashsyarof, H. L. (2024). Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia. *Dinamika Jurnal Ilmiah Hukum*, *30*(1), 9676. jim.unisma.ac.id/index.php/jdh/article/view/23708

Angelika Septi Rahayu, R., & Santoso, H. (2023). Analysis of Fake Face Images: Detecting the Authenticity of Manipulated Images Using Variational Autoencoder Methods and Deep Neural Network Forensics. *Sibatik Journal | Volume*, *2*(9), 2701–2726. https://publish.ojs-indonesia.com/index.php/SIBATIK

Dokku, S. R., & Kandula, D. (2021). A study on issues and challenges of information technology act 2000 in India. *Annals of Justice and Humanity*, *1*(1), 39–49. https://doi.org/10.33545/26179210.2019.v2.i1a.16

Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan. *Unes Law Review*, *1*(2), 157–171.

Europol. (2022). *Facing reality? : law enforcement and the challenge of deepfakes : an observatory report from the Europol innovation lab*. Publications Office of the European Union. https://data.europa.eu/doi/10.2813/08370

Gandrova, S., & Banke, R. (2023). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(10), 650–657. https://doi.org/10.5281/zenodo.10201140

Khusna, I. H., & Pangestuti, S. (2019). *Deepfake, Tantangan Baru Untuk Netizen*. *5*(2), 1–24.

Kusuma, E., & Arum, N. S. (2019). Memahami dan Menyikapi Kekerasan Berbasis Gender Online. *Southeast Asia Freedom of Expression Network*, 10.

Marcella, D., Yohannes, & Devella, S. (2022). Klasifikasi Penyakit Mata Menggunakan Convolutional Neural Network Dengan Arsitektur VGG-19. *Jurnal Algoritme*, *3*(1), 60–70.

Mu, J., Adrezo, M., & Haikal, A. N. (2024). Identifikasi Wajah Asli dan Buatan Deepfake

Menggunakan Metode Convolutional Neural Network. *TEKNIKA*, *13*(1), 45–50. https://doi.org/10.34148/teknika.v13i1.705

Mufid, F. L., & Hariandja, T. R. (2019). Efektivitas Pasal 28 Ayat (1) Uu Ite Tentang Penyebaran Berita Bohong (HOAX). *Jurnal RechtenS*, *8*(2), 179–198.

Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. *UPGRADE : Jurnal Pendidikan Teknologi Informasi*, *1*(2), 67–72. https://doi.org/10.30812/upgrade.v1i2.3702

No, V., Desember, J., Kadek, N., & Ika, D. (2024). *Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif*. *2*(1), 603–608.

Noval, S. M. R. (2019). Perlindungan Terhadap Korban Penyalahgunaan Teknik Deepfake Terhadap Data Pribadi. *Prosiding Seminar Nasional Penelitian & Pengabdian Kepada Masyarakat*, 13–18.

Nwosu, C. C., Obalum, D. C., & Ananti, M. O. (2024). Artificial intelligence in public service and governance in Nigeria. *Journal of Governance and Accountability Studies (JGAS)*, *4*(2), 109–120.

Oktallia, V., & Ariana, I. G. P. (2022). Perlindungan Terhadap Korban Penyalahgunaan Teknik Deepfake Terhadap Data Pribadi. *Jurnal Kertha Desa*, *10*(11), 1252–1263.

Putra, I. H. (2023). Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan. *UNJA Journal of LegalStudies*, *01*(2), 110–128.

Raharja, I. V. (2019). Bijak Menggunakan Media Sosial Di Kalangan Pelajar Menurut UndangUndang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *JURNAL SELAT*, *6*(2), 235–246.

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan SibeR. *Jurnal Kultura*, *1*(1), 89–97.

Roy, S. (2022). Cybercrime and islamic law: Revisiting the advantageous and hiatus horizon(s). *Annals of Justice and Humanity (AJH)*, *1*(2), 93–99.

Sahatatua, R., Gusmaria, Y., Astawa, I. K., Suherman, A. M., Setiady, T., & Tinambunan, W. D. (2024). Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum. *Journal of Multidisciplinary Academic and Practice Studies*, *2*(3), 261–265. https://doi.org/10.35912/jomaps.v2i3.2219

Setiawan, M. N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3) dilihat dari Sosio-Politik Hukum Pidana Indonesia. *Datin Law Journal*, *2*(1), 1–21.

Somers, M. (2020). *Deepfakes, explained*. MIT Sloan. mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

Song, D. (2019). *A Short History of Deepfakes*. Medium. medium.com/@songda/a-short-history-of-deepfakes-604ac7be6016

Spivak, R. (2019). Deepfakes: The newest way to commit one of the oldest crimes. *George Town Technology Review*, *3.2*, 340. georgetownlawtechreview.org/deepfakes-the-newest-way-to-commit-one-of-the-oldest-crimes/GLTR-05-2019/

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *INNOVATIVE: Journal Of Social Science Research*, *3*(2), 4208–4221.

Syaputra, R. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (Ai) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Respublica*, 5–12. https://journal.unilak.ac.id/index.php/Respublica

Tambun, Y. V., Sianturi, M. S., Theodora, K. I., Rianto, S., & Tambunan, H. (2024). Analisis Eksistensi Teknologi Deepfake terhadap Keamanan Komunikasi Digital. *Jurnal Pendidikan Tambusai*, *8*, 14485–14492.

Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis Hukum terhadap Upaya Pencegahan Kasus Deepfake Porn dan Pendidikan Kesadaran Publik di Lingkungan Digital. *Jurnal Pendidikan Tambusa*, *7*(3), 26179–26188.

Wibowo, M. H., & Fatimah, N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT(Jurnal of Education and Information Communication Technology)*, *1*, 1–5.

Yunanda, V., Wiranata, I. G. A., Agustin, Y., Rohaini, R., & Zazili, A. (2024). The Urgency of Establishing LPPDP as an Effort to Strengthen Personal Data Protection: A Comparison between

Indonesia, Hong Kong and Singapore. *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia*, *4*(1), 11–25. https://doi.org/10.35912/jihham.v4i1.2962