

TINJAUAN YURIDIS TERHADAP PENGGUNAAN TEKNOLOGI DEEPAKE UNTUK PORNOGRAFI MELALUI ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA**Sabrina Nur Syahirah¹, Bayu Prasetyo²**^{1,2}Universitas Muhammadiyah Kalimantan Timur2111102432109@umkt.ac.id¹, bp996@umkt.ac.id²

ABSTRACT; *Artificial Intelligence (AI) or artificial intelligence especially in the misuse of deepfake for pornography. The development of technology that continues to grow provides convenience. However, behind the advancement of technology presents legal challenges, especially regarding the misuse of AI technology that can manipulate faces, voices, or audio visuals using a person's personal data for pornographic purposes which of course harms the victim. In this study, using normative legal research to examine various existing regulations including the Criminal Code (KUHP), the Electronic Transaction Information Law, the Pornography Law, and the Personal Data Protection Law and their criminal liability. The results of the study show that although there are regulations governing pornography and personal data protection, there are still legal gaps and weaknesses in their implementation. Therefore, efforts are needed to strengthen regulations and increase collaboration between the government and lawmakers to prevent and reduce crimes through cyberspace like this. This study aims to determine the use of artificial intelligence, namely deepfake, in the creation and distribution of pornographic content and to provide a deeper understanding of how legal regulations in Indonesia can be applied in dealing with the misuse of this technology, and to what extent existing provisions are able to protect victims from crimes involving deepfake technology. It is hoped that this study can provide input in strengthening the legal framework related to AI and protecting the rights of its victims.*

Keywords: *Artificial Intelligence, Criminal Liability, Manipulation.*

ABSTRAK; Perkembangan teknologi yang terus berkembang memberikan kemudahan. Namun, dibalik kemajuan teknologi menghadirkan tantangan hukum, khususnya mengenai penyalahgunaan teknologi AI yang dapat memanipulasi wajah, suara, maupun audio visual menggunakan data pribadi seseorang untuk tujuan pornografi yang tentunya merugikan korban yaitu penyalahgunaan *deepfake* untuk pornografi. Dalam kajian ini, menggunakan penelitian yuridis normatif untuk mengkaji berbagai regulasi yang ada termasuk Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi Transaksi Elektronik, Undang-Undang Pornografi, dan Undang-Undang Perlindungan Data Pribadi serta pertanggungjawaban pidananya. Hasil penelitian menunjukkan bahwa meskipun telah ada aturan yang mengatur tentang pornografi dan perlindungan data pribadi, masih terdapat kekosongan hukum serta kelemahannya dalam penerapannya. Oleh karena itu, diperlukan upaya untuk memperkuat regulasi serta meningkatkan

kolaborasi antara pemerintah, dan pembuat undang-undang untuk mencegah serta mengurangi kejahatan melalui dunia maya seperti ini. Penelitian ini bertujuan untuk mengetahui penggunaan kecerdasan buatan yaitu *deepfake* pada pembuatan dan penyebaran konten pornografi serta memberikan pemahaman yang lebih mendalam tentang bagaimana pengaturan hukum di Indonesia dapat diterapkan dalam menangani penyalahgunaan teknologi ini, serta sejauh mana ketentuan yang ada saat ini mampu melindungi korban dari kejahatan yang melibatkan teknologi *deepfake*. Diharapkan studi ini dapat memberikan masukan dalam memperkuat kerangka hukum terkait AI dan melindungi hak-hak korbannya.

Kata Kunci: Kecerdasan Buatan, Manipulasi, Pertanggungjawaban Pidana.

PENDAHULUAN

Di era yang berkembang pesat ini, kemajuan teknologi telah berubah secara drastis. Semua aktivitas yang dulunya kita lakukan dengan cara konvensional kini telah beralih ke digital. Dengan perkembangan zaman menuju era digitalisasi, semua aspek kehidupan kita menjadi lebih mudah. Kita dapat melakukan semua pekerjaan dengan lebih cepat.¹ Perkembangan pesat teknologi informasi di era digital telah melahirkan inovasi, salah satunya adalah kecerdasan buatan atau *artificial intelligence* (AI). Menurut informasi dari Databoks, pada tahun 2023, Indonesia menempati posisi ketiga dalam penggunaan kecerdasan buatan di dunia (AI), dengan total 1,4 miliar kunjungan pada AI, yang berkontribusi sebesar 5,60% dari total traffic.² Kemunculan AI menjadi bukti nyata bahwa teknologi dapat memberikan kontribusi yang memberikan kemudahan bagi kehidupan manusia. Namun, dibalik kemudahan juga membawa dampak negatif yang kompleks, salah satunya dalam bentuk penyalahgunaan teknologi untuk kejahatan dunia maya.

Salah satu teknologi yang mendapat sorotan luas adalah *deepfake*. *Deepfake* merupakan bagian dari kecerdasan buatan. Menurut etimologi, *deepfake* dalam bahasa Inggris dari gabungan kata "*deep learning*" dan "*fake*".³ Sebagai bagian dari AI, *deepfake* menggunakan penggunaan algoritma yang dapat menyesuaikan dengan semakin banyaknya data yang diproses. *Deep learning* memungkinkan pengembangan perangkat lunak yang mampu

¹ Bayu Prasetyo, Dkk. *Reconstruction Of Personal Data Protection Law Againsts Data Leakage In The Digitalization Era After The Covid-19 Pandemic*, Lembuswana Law Review: Public Law, Civil Law, Business Law, Vol. 1 No. 1, Juni 2023, hal, 79.

² Databoks, Indonesia Penyumbang Kunjungan Aplikasi AI Terbanyak ke-3 di Dunia, dalam <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/a49ed3eb121983b/indonesia-penyumbang-kunjungan-ai-terbanyak-ke-3-di-dunia>, Diakses pada 31 Januari 2024, 13: 23 WIB.

³ Ramadhan, Dwi Galih, *Perlindungan Hukum Atas Investasi Artificial Intelligence Di Era Revolusi Industri 4.0 & Society 5.0*, Universitas Islam Indonesia, 2022.

menghasilkan *deepfake*. Adapun kata "fake" pada *deepfake* menunjukkan bahwa media yang dihasilkan adalah palsu, bukan yang sebenarnya. *Deepfake* mampu memanipulasi fitur wajah seseorang dengan memanfaatkan teknologi kecerdasan buatan.⁴ Jadi, Melalui *deepfake*, seseorang bisa mengganti wajah dalam video, membuat suara tiruan, dan menciptakan objek tiga dimensi sehingga tidak lagi akurat dan tidak berdasarkan pada realitas. Hal ini membuka peluang untuk membuat konten visual yang sangat kreatif, namun juga berpotensi disalahgunakan.

Deepfake awalnya digunakan untuk hiburan dan mempermudah pekerjaan, namun kini sering disalahgunakan untuk menipu dan menyebarkan informasi palsu dengan memanipulasi gambar dan audio-visual. Meskipun memiliki manfaat dalam industri kreatif, penyalahgunaannya untuk membuat konten pornografi tanpa persetujuan telah menimbulkan masalah hukum yang serius. Berdasarkan survey yang dilakukan oleh deepttrace pada tahun 2019, sebanyak 96% dari konten *deepfake* video yang beredar bermuatan pornografi.⁵ Salah satu contoh nyata penyalahgunaan teknologi *deepfake* pornografi yang menimbulkan kekhawatiran publik terjadi di beberapa negara, termasuk Indonesia. Dimana beberapa publik figur menjadi korban dari teknologi ini, termasuk para selebriti tanah air. Fenomena ini tidak hanya mencemarkan nama baik dan melanggar hak privasi korban, tetapi juga menghadirkan tantangan serius bagi penegakan hukum di Indonesia, mengingat pengaturan yang ada belum secara spesifik mengatur tentang teknologi tersebut.

Di Indonesia, maraknya kasus *deepfake* pornografi berkaitan dengan pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, serta Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ITE pada Pasal 27 ayat (1) menegaskan melarang penyebaran informasi elektronik yang melanggar kesusilaan, sementara Undang-Undang Pornografi pada Pasal 4 ayat (1) mengatur larangan produksi, penyebaran, dan konsumsi konten pornografi.⁶ UU PDP menetapkan kewajiban bagi penyelenggara sistem elektronik untuk menjaga keamanan data pribadi penggunanya, termasuk pengumpulan, penyimpanan, dan pemrosesan data. Meskipun perundang-undangan mengatur penyebaran konten elektronik yang tidak pantas dan pornografi, teknologi *deepfake* menghadirkan tantangan baru. Regulasi yang ada belum secara eksplisit mengatur mengenai kecerdasan

⁴ Nibert Young, *DeepFake Technology: Complete Guide to Deepfakes*, Politics and Social Media United States, 2019.

⁵ Rahayu dan Santoso, *Analisis Gambar Wajah Palsu: Mendeteksi Keaslian Gambar Yang Dimanipulasi Menggunakan Metode Variational Autoencoder Dan Forensics Deep Neural Network*, Sibatik Jurnal, hal. 47.

⁶ Damarjati, *Fenomena Deepfake dan Tantangan Hukum Siber di Indonesia*, Jurnal Hukum dan Teknologi Informasi, Vol. 5 No. 1, hal. 46.

buatan, seh menciptakan celah hukum yang dapat dimanfaatkan pelaku kejahatan untuk mengeksploitasi teknologi ini tanpa aturan hukum yang kuat.

Kekosongan hukum merujuk pada tidak adanya peraturan yang mengatur secara khusus mengenai penyalahgunaan teknologi kecerdasan buatan ini, yang menyebabkan ketidakpastian hukum dan minimnya perlindungan yang menyebabkan kerugian yang signifikan bagi individu yang menjadi korban, karena mereka tidak memiliki perlindungan yang memadai terhadap penyalahgunaan data pribadi mereka. Kurangnya pemahaman dan kesadaran di kalangan masyarakat dan penegak hukum mengenai risiko dan dampak dari teknologi *deepfake* juga memperburuk situasi. Hal ini menunjukkan perlunya penguatan kebijakan dan regulasi yang lebih komprehensif untuk menghadapi dan menyelesaikan masalah yang muncul akibat perkembangan teknologi ini. Karenanya, penting bagi pemangku kepentingan untuk segera merumuskan regulasi yang jelas dan efektif mengenai penggunaan teknologi AI, khususnya *deepfake* pornografi. Tujuannya adalah agar tercipta ruang digital yang lebih terlindungi bagi setiap orang serta menghormati privasi serta hak asasi manusia.

Fenomena ini menunjukkan adanya kesenjangan dalam pengaturan hukum positif di Indonesia dalam mengantisipasi kemajuan teknologi. Aparat penegak hukum sering kali mengalami kesulitan dalam menghadapi dan mengusut tuntas kasus *deepfake* karena proses pengumpulan bukti serta identifikasi pelaku dapat menjadi lebih rumit dibandingkan dengan kasus pornografi konvensional. Kesulitan ini semakin diperburuk dengan fakta bahwa *deepfake* memungkinkan pelaku untuk tetap anonim, membuat upaya pelacakan dan penuntutan menjadi semakin kompleks. Urgensi untuk menganalisis penggunaan teknologi *deepfake* pornografi semakin meningkat seiring dengan semakin meningkatnya peristiwa yang terjadi. Dengan demikian, penelitian ini diharapkan mampu memberikan rekomendasi yang berguna untuk menciptakan lingkungan digital yang lebih aman dan menghormati privasi serta hak asasi manusia.

Beberapa penelitian lain tentang kecerdasan buatan memiliki kesamaan dengan topik penelitian ini. Pertama, penelitian yang disusun oleh Adzhar Anugerah Trunapasha, Dkk. Penelitian tersebut berfokus membahas regulasi AI yang dilakukan kepada tokoh masyarakat serta mengenai penyalahgunaan *artificial intelligence* secara umum. Sedangkan, penelitian ini lebih fokus membahas tentang *deepfake* pornografi yang korbannya masyarakat umum serta menjelaskan aturan hukum yang relevan serta pertanggungjawaban pidana terhadap pelakunya. Selanjutnya, penelitian oleh Itok Dwi Kurniawan, pada penelitian menyimpulkan

bahwa kecerdasan buatan tidak dapat dianggap sebagai subjek hukum karena tindakannya semata-mata merupakan implementasi dari perintah penggunanya. Selain itu, kajian ini berfokus menyoroti status AI sebagai subjek hukum, tidak merumuskan tentang pengaturan hukum terkait tindak pidana tersebut. Sedangkan penelitian ini membahas mengenai penyalahgunaan *deepfake* untuk pornografi serta aturan hukum di Indonesia terkait *deepfake* pornografi. Ketiga adalah penelitian Muhammad Ariq Abir Jufri dan Akbar Kurnia, Penelitian tersebut mengkaji aspek hukum internasional terkait penggunaan *deepfake* pada kaitannya dengan perlindungan data pribadi dan dampaknya. Namun, penelitian tersebut hanya menjelaskan kasus *deepfake* dalam aspek internasional. Sedangkan, penelitian ini akan membahas mengenai pengaturan mengenai penyalahgunaan *deepfake* pornografi dalam aspek hukum di Indonesia.

Dengan demikian, meskipun ada kesamaan dalam tema yang diangkat, setiap penelitian memberikan kontribusi terhadap pemahaman isu-isu hukum yang berkaitan dengan teknologi *artificial intelligence*. Penelitian ini bertujuan untuk mengetahui penggunaan kecerdasan buatan yaitu *deepfake* pada pembuatan dan penyebaran konten pornografi serta memberikan pemahaman yang lebih mendalam mengenai bagaimana pengaturan hukum di Indonesia dapat diterapkan dalam menangani penyalahgunaan teknologi ini, serta sejauh mana ketentuan yang ada saat ini mampu melindungi korban dari kejahatan yang melibatkan teknologi *deepfake*.

METODE PENELITIAN

Pada metode penelitian ini menggunakan jenis penelitian yuridis normatif, berfokus pada analisis penerapan aturan-aturan hukum pada hukum positif. Berdasarkan pada bahan hukum primer, sekunder, dan tersier. Menggunakan pendekatan perundang-undangan yang dilakukan dengan memahami peraturan perundang-undangan melalui penafsiran terhadap hierarki dan prinsip-prinsip yang terkandung dalam peraturan tersebut dengan proses menganalisa suatu peraturan atau regulasi Penelitian ini terkait dengan permasalahan yang sedang dihadapi dan relevan dengan isu hukum mengenai penelitian. Serta menggunakan pendekatan konseptual untuk menganalisisnya berdasarkan pandangan dan doktrin yang ada pada ilmu hukum. Pendekatan ini diterapkan untuk memberikan argumen atau rekomendasi terkait isu pornografi yang menggunakan teknologi *deepfake*, sebagai salah satu bagian dari kemajuan teknologi kecerdasan buatan.

HASIL DAN PEMBAHASAN**3.1 Analisis Yuridis Terhadap Penggunaan Teknologi Deepfake Untuk Pornografi**

Sebagai negara hukum, Indonesia telah menetapkan undang-undang yang berkaitan dengan pornografi, Penggunaan teknologi deepfake yang semakin marak menimbulkan berbagai dampak negatif, salah satunya adalah dalam bentuk penyalahgunaan untuk pornografi. Teknologi ini memungkinkan manipulasi gambar dan video seseorang tanpa izin, yang kemudian dapat disebarluaskan untuk merusak reputasi atau digunakan sebagai alat pemerasan. Dalam analisis dari peraturan perundang-undangan ada beberapa peraturan yang harus dipahami antara lain:

1. Undang-Undang Dasar 1945

Landasan hukum tertinggi tercantum pada Pembukaan Undang-Undang Dasar 1945 Negara Republik Indonesia, yang melindungi seluruh bangsa dan tumpah darah Indonesia, perlindungan hak privasi kemudian diperkuat dalam Pasal 28G ayat (1) UUD 1945⁷. Pasal ini secara eksplisit menjamin hak setiap orang untuk dilindungi atas diri pribadi, keluarga, kehormatan, martabat, harta benda, dan jaminan rasa aman. Dengan demikian, hak privasi diakui sebagai hak asasi yang fundamental, dan perlindungan data pribadi menjadi bagian tak terpisahkan darinya. UUD 1945 menjadi sumber dan landasan bagi peraturan-peraturan di bawahnya yang mengatur privasi dan data pribadi. Berdasarkan ketentuan tersebut menegaskan bahwa kejahatan deepfake pornografi bertentangan terhadap hak asasi manusia. Dengan demikian, dapat disimpulkan negara bertanggung jawab untuk menjamin perlindungan hak asasi manusia setiap warganya, termasuk hak atas privasi dan martabat, terlindungi dari ancaman kejahatan siber yang semakin canggih seperti penyalahgunaan teknologi deepfake.

2. Kitab Undang-Undang Hukum Pidana (KUHP)

Penyalahgunaan deepfake pornografi di Indonesia dapat dianggap sebagai tindak pidana terhadap kesusilaan. sesuai ketentuan KUHP, yang mencakup beberapa pasal terkait pelanggaran kesusilaan dan pencemaran nama baik. Pasal 281 KUHP mengatur pidana bagi pelaku pelanggaran kesusilaan, bagi mereka yang dengan sengaja dan secara terbuka melanggarkesusilaan. Meskipun pasal ini menjadi landasan hukum dalam penanganan kasus terkait, rumusannya masih umum dan tidak jelas mengenai bentuk pelanggaran kesusilaan, terutama dalam membedakan tindakan langsung dan tidak langsung, seperti melalui

⁷ Upik Mutiara & 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, hal. 44.

media. Sementara itu, Pasal 310 KUHP mengatur pelanggaran pencemaran nama baik. Pada konteks deepfake pornografi, manipulasi wajah seseorang ke dalam konten pornografi tanpa persetujuan dapat dianggap sebagai pencemaran nama baik dan pelanggaran kehormatan individu. Pasal ini sering dijadikan dasar hukum untuk kasus pencemaran nama baik di Indonesia. Walaupun demikian, berdasarkan Putusan MK No. 78/PUU-XXI/2023, ketentuannya dinyatakan inkonstitusional secara bersyarat.⁸ Mahkamah Agung berpendapat bahwa ketentuan ini masih konvensional dan tidak efektif menangani pencemaran nama baik dalam dunia maya, karena syarat "di muka umum" dianggap kurang memadai dan menyulitkan penerapannya di internet. Dengan demikian, diperlukan rumusan hukum yang lebih luas dan adaptif terhadap karakteristik dunia maya.

3. Undang-Undang No. 12 Tahun 2005 tentang Pengesahan International Covenant On Civil And Political Rights

Perlindungan privasi merupakan aspek penting yang diatur dalam hukum internasional, khususnya melalui International Covenant on Civil and Political Rights (ICCPR) yang diratifikasi oleh Indonesia melalui Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan Kovenan Internasional tentang Hak-Hak Sipil dan Politik. Dalam konteks ini, teknologi yang berkembang pesat, seperti deepfake, menimbulkan tantangan serius terhadap hak privasi yang dijamin dalam Pasal 17 ICCPR.⁹ Deepfake yang memanipulasi gambar dan video untuk menciptakan konten yang tampak nyata, berpotensi melanggar hak privasi individu dengan cara yang sangat merugikan. Misalnya, penggunaan deepfake untuk membuat konten pornografi tanpa persetujuan individu yang terlibat tidak hanya mengganggu privasi mereka, tetapi juga dapat merusak reputasi dan kehormatan mereka secara signifikan. Pasal 17 ICCPR secara eksplisit melarang tindakan sewenang-wenang yang dapat mengganggu privasi, keluarga, dan tempat tinggal seseorang, serta merusak kehormatan dan reputasi individu.

4. Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (TPKS)

Pengaturan ini mengklasifikasikan kekerasan seksual melalui media elektronik sebagai Kekerasan Seksual Berbasis Elektronik (KSBE). UU TPKS Pasal 14 Ayat (1) mengatur tiga

⁸ Jennifer Angelina & Listyowati Sumanto, *Kajian Yuridis Kasus Pencemaran Nama Baik Berdasarkan KUHP yang Berkepastian Hukum*, Journal of Accounting Law Communication and Technology, Vol. 2 No. 1, 2025, hal. 513.

⁹ Jeremiah Maximillian Laza & Rizky Karo Karo, *Perlindungan Hukum Terhadap Artificial Intelligence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR*, Lex Prospicit, Vol. 1 No. 2, 2023

jenis kekerasan seksual berbasis elektronik. Pertama, tindakan merekam atau mengambil gambar seksual tanpa izin. Kedua, pengiriman informasi atau dokumen seksual elektronik tanpa izin. Ketiga, penguntitan atau pelacakan elektronik untuk tujuan seksual. Pelaku ketiga tindakan ini dapat dihukum atas kekerasan seksual berbasis elektronik. Terdapat perbedaan antara UU Pornografi dan UU TPKS, di mana UU TPKS mengadopsi konsep konsensualitas dengan frasa "di luar kehendak atau tanpa persetujuan" dalam rumusannya, sedangkan UU Pornografi tidak mengenal konsep ini, sehingga semua tindakan dapat dikenakan sanksi pidana. Meskipun UU TPKS mengatur KSBE, manipulasi gambar untuk membuat deepfake pornografi belum diatur, menciptakan kekosongan hukum.

5. Undang-Undang No. 44 tahun 2008 tentang Pornografi

Pasal 1 angka 1 UU Pornografi mendefinisikan bahwa konten pornografi yang dihasilkan melalui teknologi deepfake selain melanggar hukum, tetapi juga berpotensi merusak prinsip moral dan etika masyarakat. Namun, terdapat ketidakjelasan dalam definisi pornografi akibat multitafsir dalam implementasi Pasal 1 angka 1 jo. Pasal 4 UU Pornografi. Oleh karena itu, hakim memiliki peran penting dalam menilai apakah suatu tindakan dapat dikategorikan sebagai pornografi. Dalam konteks deepfake pornografi, individu yang menciptakan konten tersebut dapat dijerat berdasarkan undang-undang ini. Menurut Pasal 4 ayat (1) UU Pornografi, suatu perbuatan dapat dikategorikan sebagai tindak pidana pornografi apabila memenuhi unsur meliputi kesalahan "yang dilakukan dengan sengaja", tindakan melawan hukum "tanpa hak", perbuatan "seperti memproduksi, menyebarluaskan, dan lain-lain", serta objek "pornografi".¹⁰ Namun, UU Pornografi belum secara eksplisit mengatur penggunaan teknologi digital seperti deepfake untuk pornografi, sehingga menyebabkan timbulnya celah dalam peraturan yang dapat digunakan oleh pelaku untuk menghindari pertanggungjawaban.

6. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Ketentuan dalam Pasal 27 ayat (1) memiliki kaitan erat dengan perlindungan data pribadi sebagai bagian dari hak asasi pribadi. UU ITE juga menjadi landasan hukum dalam penegakan hukum terhadap kasus deepfake pornografi yang disebarkan melalui internet. Berdasarkan pasal tersebut, seseorang yang mendistribusikan, mentransmisikan, atau membuat Informasi atau dokumen elektronik yang melanggar kesusilaan dan disebarluaskan dengan sengaja serta

¹⁰ Brolin Rongkene, Tindak Pidana Pornografi Menurut Kuhp Dan Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi, *Lex Crimen*, Vol. 9, No. 1, Maret 2020, hal. 112.

tanpa hak dapat dipidana dan dimintai pertanggungjawaban secara hukum.¹¹ Namun, rumusan tersebut menimbulkan berbagai tafsir terkait tidak adanya kejelasan mengenai definisi "informasi elektronik atau dokumen elektronik yang melanggar kesusilaan." Barda Nawawi mengemukakan bahwa Undang-Undang Khusus idealnya tidak hanya memuat rumusan tindak pidana, tetapi juga aturan-aturan khusus yang melengkapinya sebagai payung hukum.

Selanjutnya pada pasal 27A UU ITE menegaskan bahwa "Setiap Orang yang sengaja menyerang kehormatan atau nama baik orang lain dengan menuduhkan suatu hal untuk diketahui umum dalam bentuk Informasi Elektronik dan/atau Dokumen Elektronik melalui Sistem Elektronik" sangat penting sebagai pelengkap Pasal 310 KUHP. Pengaturan ini diperlukan karena karakteristik media elektronik yang khas dan lintas batas. Meskipun unsur-unsur dalam kedua pasal tersebut pada dasarnya sama, Pasal 27A UU ITE tidak menciptakan perubahan dalam norma hukum pidana, melainkan menegaskan unsur tambahan yang spesifik terkait perkembangan dan penggunaan di bidang elektronik.¹²

Penyalahgunaan teknologi deepfake sejalan dengan Pasal 28 ayat (1) UU ITE, yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik." "Setiap orang" merujuk pada pelaku penyalahgunaan deepfake pornografi, "dengan sengaja dan tanpa hak" berarti memanipulasi data pribadi orang lain dengan hasil video yang mengandung unsur pornografi, dan "menyebarkan berita bohong dan menyesatkan" berarti menyebarkan konten pornografi hasil manipulasi deepfake yang tidak benar, yang merugikan konsumen dan merusak citra serta reputasi korban.

Selanjutnya pada Pasal 35 UU ITE memuat aturan secara spesifik mengenai tindakan manipulasi informasi dan/atau dokumen elektronik. "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." Peraturan ini secara tegas melarang manipulasi terhadap data atau dokumen digital agar dianggap otentik, yang sangat relevan dalam konteks deepfake. Manipulasi gambar atau video

¹¹ L. Heru Sujamawardi, *Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Dialogia Iuridica Jurnal Hukum Bisnis dan Investasi, Vol. 9 No. 2, April 2018, hal. 89.

¹² Mahkamah Konstitusi Republik Indonesia, *DPR: Ketentuan Pidana dalam UU ITE Diatur dalam KUHP Nasional*, dalam <https://www.mkri.id/index.php?page=web.Berita&id=19637>, Diakses Pada 31 Januari 2024

dengan teknologi deepfake bertujuan untuk menciptakan representasi palsu yang tampak nyata, sehingga memenuhi unsur manipulasi yang dimaksud dalam pasal ini.

Namun, Pada regulasi dalam UU ITE yang berlaku saat ini hanya mengatur AI sebagai agen elektronik yang melaksanakan tindakan terhadap informasi elektronik secara otomatis, belum secara eksplisit mengatur aspek-aspek substantif seperti etika, privasi, dan konsekuensi yang melekat pada penggunaan AI. Tidak adanya kerangka hukum yang jelas dan komprehensif yang mengatur proses penggunaan kecerdasan buatan menimbulkan ketidakpastian terkait pertanggungjawaban hukum dari penyalahgunaan teknologi tersebut.

7. Undang-Undang Perlindungan Data Pribadi

Perlindungan data pribadi bertujuan untuk melindungi hak dan privasi individu atas informasi dan data mereka, sehingga tidak dapat diakses oleh pihak yang tidak berhak.¹³ Dalam konteks penyalahgunaan teknologi deepfake, objek tindak pidana adalah data pribadi korban. Teknologi deepfake AI memungkinkan penggunaan informasi dan gambar wajah, yang termasuk dalam data biometrik khusus. Deepfake yang menggambarkan individu termasuk dalam kategori data pribadi karena memiliki kaitan erat dengan identified or identifiable natural person.¹⁴ Meskipun UU PDP tidak secara langsung mengatur AI atau deepfake, karena AI menggunakan data, UU PDP secara tidak langsung memberikan perlindungan hukum terhadap deepfake ilegal yang mengambil data pribadi tanpa persetujuan. Dengan demikian, penyalahgunaan deepfake dapat dianggap sebagai pelanggaran privasi.

Pasal 65 ayat (1) UU PDP "Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya untuk keuntungan diri sendiri atau orang lain yang dapat merugikan Subjek Data Pribadi." Pasal ini menekankan perlindungan data pribadi dengan melarang pengumpulan ilegal data orang lain, mencerminkan komitmen untuk menjaga privasi dan mencegah penyalahgunaan data. Oleh karena itu, individu dilarang mengumpulkan data pribadi yang bukan haknya secara ilegal, yang dapat merugikan pemilik data.

Pasal 65 ayat (3) menyatakan, "Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya." Pasal ini melindungi hak individu atas data

¹³ Stanley K Laughlin, "Westin: Privacy and Freedom Westin: Privacy and Freedom Recommended Citation Recommended Citation", Michigan Law Review, Vol. 66.

¹⁴ Jeremi ah Maximillian Laza & Rizky Karo Karo, *Op.Cit.*

pribadinya dengan melarang penggunaan data tersebut oleh pihak lain tanpa izin, menunjukkan bahwa individu memiliki hak atas data pribadinya dan penggunaannya harus dengan persetujuan yang jelas. Hal ini mencerminkan prinsip transparansi dan akuntabilitas dalam pengelolaan data pribadi. Selanjutnya, Pasal 66 Pasal: “Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain” Pasal ini juga mengatur larangan pembuatan atau pemalsuan data pribadi, yang menunjukkan bahwa integritas data pribadi sangat penting.

Berdasarkan pembahasan sebelumnya, dapat ditarik kesimpulan bahwa karakteristik AI berdasarkan UU ITE, terdapat kemiripan dengan "Agen Elektronik". Berdasarkan Pasal 1 angka 8 UU ITE, 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.

Sejauh ini perlindungan hukum terhadap korban kejahatan deepfake pornografi telah diatur dengan beberapa ketentuan di dalam peraturan yang tersedia, namun ketentuan tersebut dapat dikaitkan karena kejahatan deepfake pornografi memiliki muatan konten seksual dan penyalahgunaan data pribadi. Tindakan ini dapat dianggap sebagai tindak pidana siber (cyber crime) karena telah memenuhi syarat yang telah diatur dalam hukum positif Indonesia. Namun, hukum positif di Indonesia belum cukup kuat untuk menjerat pelaku karena peraturan yang ada, seperti KUHP, UU Pornografi, UU ITE, dan UU PDP, belum mengatur secara jelas dan rinci tentang tindak pidana ini, terutama karena tidak ada kata "kecerdasan buatan" atau "artificial intelligence" yang secara eksplisit disebutkan dalam peraturan tersebut.

Dalam konteks digital, UU ITE dapat dianggap sebagai payung hukum yang mengatur berbagai aspek, hanya beberapa ketentuan dalam UU ITE yang relevan dengan penyalahgunaan teknologi deepfake. UU ITE hadir dengan tujuan memberikan perlindungan hukum terhadap data pribadi dalam era digital, serta mengatur berbagai tindak pidana yang memanfaatkan teknologi elektronik sebagai sarana kejahatan, termasuk pornografi yang

dilakukan melalui media elektronik. Hukum pidana terkait pornografi awalnya tercantum dalam KUHP dan kemudian diatur lebih lanjut dalam UU Pornografi. Namun, dengan berkembangnya teknologi dan penggunaan media elektronik sebagai sarana penyebaran, oleh karena itu, dibentuklah UU ITE.

Akan tetapi, UU ITE hanya memiliki ketentuan yang terbatas tentang perlindungan data pribadi, tanpa memberikan pengaturan yang lebih spesifik dan komprehensif, sehingga menyebabkan minimnya perlindungan bagi masyarakat akibat pengaturan hukum yang lemah. Meskipun mengatur berbagai kegiatan informasi dan transaksi elektronik di dunia digital, tetapi tidak cukup kuat untuk menangani risiko penggunaan AI tingkat tinggi, contohnya deepfake. UU ini belum memiliki ketentuan khusus terkait teknologi tersebut, seperti manipulasi dan penyebaran hoaks. Terdapat celah dalam UU ITE terkait etika penggunaan AI, termasuk tanggung jawab pengembang dan pengguna deepfake.

Terkait perlindungan data pribadi, Indonesia memiliki dasar hukum yang kuat, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.¹⁵ Akan tetapi juga tidak secara eksplisit mengatur penyalahgunaan teknologi tersebut. Walaupun UU PDP mengatur pidana pemalsuan data biometrik, namun belum ada ketentuan yang mengatur pertanggungjawaban pidana terkait deepfake pornografi. Hal ini menyebabkan adanya celah hukum.

Berlandaskan pada peraturan perundang-undangan yang berlaku di Indonesia, perbuatan menyimpang yang melanggar hukum pada penggunaan teknologi AI, khususnya deepfake pornografi, belum diatur secara spesifik. Namun, hukum positif di Indonesia memiliki dasar hukum untuk menangani kasus ini, dengan UU ITE sebagai peraturan terbaru dan paling khusus untuk tindak pidana siber. Prinsip “Lex Specialis derogat legi generali” menegaskan bahwa hukum khusus mengesampingkan hukum umum, sementara “Lex posterior derogat legi priori” menegaskan bahwa hukum terbaru mengesampingkan yang lama. UU ITE berfungsi sebagai “Lex Specialis” dan “Lex Posterior” yang paling sesuai untuk mengatur penyalahgunaan AI. Karena UU ITE secara khusus mengatur transaksi elektronik, undang-undang ini dapat digunakan untuk menangani penyebaran konten deepfake yang mengandung unsur pornografi, pelecehan, atau pencemaran nama baik. Namun, mengingat unsur-unsur

¹⁵ Bella Christine & Christine S.T. Kansil, *Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, Syntax Literate: Jurnal Ilmiah Indonesia, Vol. 7, No. 09, September 2022, hal. 3.

dalam deepfake pornografi juga termasuk dalam tindak pidana pornografi, pengaturannya melibatkan UU ITE dan UU Pornografi.

Berdasarkan penjelasan sebelumnya, dapat ditarik kesimpulan bahwa pelaku penyalahgunaan deepfake pornografi dapat dijerat dengan UU ITE dalam Pasal 27 ayat (1) dimana unsur pidana pelaku menyebarluaskan atau mentransmisikan konten deepfake pornografi dalam platform elektronik. UU Pornografi Pasal 4 ayat (1) dimana unsur pidananya adalah pembuatan konten deepfake pornografi dapat dikategorikan sebagai bentuk produksi pornografi, meskipun menggunakan teknologi manipulatif seperti deepfake. Pembuatan dan penyebaran konten video pornografi juga dapat dianggap sebagai tindakan yang melanggar kehormatan serta repuasi seseorang “pencemaran nama baik” dan diketahui oleh umum dalam pasal 310 ayat (2) KUHP. Konten video pornografi secara nyata merusak reputasi orang lain.

Berdasarkan analisis yuridis ini menunjukkan bahwa kehadiran teknologi deepfake memberikan tantangan serius bagi sistem hukum di Indonesia, karena dari aturan yang ada di dalam perundang-undangan tersebut belum jelas adanya yang mengatur mengenai kejahatan deepfake yang berisikan konten pornografi atau tidak. Karenanya, penting bagi pemerintah untuk memperbarui atau membuat regulasi spesifik mengenai kejahatan deepfake pornografi untuk menciptakan payung hukum yang kuat. Pengaturan ini diperlukan sebagai alat untuk perkembangan masyarakat, mengingat Indonesia adalah negara hukum sesuai Pasal 1 ayat (3) UUD NRI 1945.¹⁶ Dikarenakan penyalahgunaan teknologi seperti deepfake pornografi telah dianggap sebagai tindak pidana, tetapi belum memiliki regulasi yang jelas, sehingga kasusnya semakin meningkat dan korban merasa terancam di dunia maya. Secara keseluruhan, penulis berpendapat bahwa meskipun AI berpotensi untuk kemajuan teknologi, perlindungan privasi data pribadi merupakan hal yang paling penting dalam pengembangan dan penerapan teknologi ini.

3.2 Pertanggungjawaban Pidana Pelaku Penggunaan Teknologi Deepfake Untuk Pornografi

Pertanggungjawaban pidana, atau criminal responsibility, merujuk pada pemidanaan pelaku untuk menentukan apakah terdakwa atau tersangka bertanggung jawab atas tindak pidana tersebut.¹⁷ Dari berbagai ketentuan dalam peraturan yang berlaku di Indonesia hingga

16 Nur Hidayat, *Rujukan Dan Aplikasi Sistem Hukum Indonesia Berdasarkan Pasal 1 Ayat (3) UUD 1945 Pasca Amandemen Ke Tiga*, Uir Law Review, Vol. 1 No. 2, Oktober 2017, hal. 192.

17 Tim Departemen Pendidikan Nasional, 2005, *Kamus Besar Bahasa Indonesia*, Pusat Bahasa Departemen Pendidikan Nasional, Balai Pustaka, Jakarta, hal.1139.

saat ini, sebenarnya telah ada landasan hukum yang dapat digunakan untuk penegakan hukum terhadap penyalahgunaan teknologi deepfake dalam konteks pornografi. Meskipun belum ada pengaturan yang tegas dan rinci mengenai hal ini, terdapat keterkaitan dengan pengaturan hukum yang relevan. Adapun perundang-undangan yang ada relevansinya dengan penyalahgunaan teknologi deepfake adalah:

1. Kitab Undang-Undang Hukum Pidana (KUHP)

Pasal 281 (Kejahatan Terhadap Kesusilaan) “Diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat juta lima ratus ribu rupiah: (1) barang siapa dengan sengaja dan terbuka melanggar kesusilaan; (2) barang siapa dengan sengaja dan di depan orang lain yang ada di situ bertentangan dengan kehendaknya, melanggar kesusilaan” Perbuatan asusila merupakan tindakan yang melanggar norma kesusilaan, khususnya yang berkaitan dengan seksual atau bagian tubuh yang dapat membangkitkan rasa malu, jijik, atau hasrat seksual.. Tanpa terpenuhinya unsur-unsur yang dipersyaratkan, suatu tindakan tidak dapat serta merta dianggap sebagai sebuah tindak pidana, yang mana unsur tindak pidana asusila adalah adanya pelaku, niat yang disengaja, dilakukan di muka umum, dan melanggar norma kesusilaan. Apabila semua unsur ini terpenuhi, pelaku dapat dikenai hukuman pidana.

Adapun dalam Pasal 310 (Pencemaran Nama Baik): “(1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat juta lima ratus rupiah. (2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat juta lima ratus rupiah.” Perbuatan “penghinaan atau pencemaran nama baik” yang dilakukan secara langsung dapat dikategorikan sebagai pelanggaran terhadap Pasal 310 ayat (1) KUHP. Sementara itu, jika perbuatan tersebut dilakukan melalui media tertulis atau gambar yang disebarkan, dipertontonkan, atau ditempelkan, maka pelaku dapat dijerat dengan Pasal 310 ayat (2) KUHP yang lebih berfokus pada pelanggaran yang tidak dilakukan secara langsung, seperti pencemaran nama baik melalui tulisan atau unggahan publik, termasuk penyalahgunaan deepfake. Unsur-unsur yang terkandung dalam tindak pidana fitnah pada pasal ini adalah, seseorang (pelaku); pelaku melakukan perbuatan mencemarkan nama baik

orang lain, baik melalui ucapan maupun tulisan; pelaku memiliki hak untuk membuktikan kebenaran dari tuduhan; pelaku tidak membuktikannya; dan tuduhan tersebut diketahuinya tidak benar.

2. Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi

Selanjutnya pada Undang-Undang Tentang Pornografi, dalam ketentuannya bagi pelaku deepfake pornografi yang membuat rekayasa gambar atau video dari wajah, tubuh, serta suara orang lain diatur dalam Pasal 29 yang menyatakan bahwa apabila seseorang melanggar ketentuan Pasal 4 Ayat (1) dapat dikenakan sanksi. “Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksud dalam Pasal 4 ayat (1) dipidana dengan pidana penjara paling singkat 6 (enam) bulan dan paling lama 12 (dua belas) tahun dan/atau pidana denda paling sedikit Rp250.000.000,00 (dua ratus lima puluh juta rupiah) dan paling banyak Rp6.000.000.000,00 (enam miliar rupiah).”

Dengan mengacu pada ketentuan pasal tersebut, pelaku bertanggung jawab secara pidana dengan memenuhi unsur-unsur, “Perbuatan” yaitu memproduksi atau membuat, dan “Objek perbuatan” yaitu pornografi. Penyalahgunaan deepfake ini dalam membuat video pornografi menggunakan deepfake dan memasukkan wajah orang lain di dalamnya, tanpa persetujuan dan sepengetahuan orang tersebut, secara tegas dilarang oleh UU Pornografi.

3. Undang-Undang tentang Informasi Dan Transaksi Elektronik Adapun dalam Undang-Undang tentang Informasi Dan Transaksi Elektronik (UU ITE)

Pasal 45 Ayat (1) menyatakan, "Setiap orang yang memenuhi unsur dalam Pasal 27 ayat (1), (2), (3), atau (4) dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1.000.000.000." Jika seseorang memenuhi kriteria yang ditentukan, maka mereka dapat diadili dan dimintakan pertanggungjawaban berdasarkan Pasal 45 ayat (1) UU ITE, yang menetapkan sanksi pidana dan denda sebagai konsekuensi. Subjek yang melakukan tindakan pidana ini adalah individu yang menyebarkan konten informasi atau dokumen elektronik yang bertentangan dengan prinsip kesusilaan. Sanksi yang diberikan dapat berupa pidana dan

denda secara bersamaan, atau salah satu dari keduanya, tergantung pada keputusan hakim yang menggunakan kata penghubung "dan/atau" sebagai dasar penentuan sanksi.¹⁸

Pasal 45A Ayat (1) menyatakan, "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik dipidana dengan penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1.000.000.000." Individu yang menyebarkan informasi palsu dapat dijerat dengan hukum, dan perbuatan tersebut harus dilakukan dengan niat jahat dan tanpa izin melalui media elektronik. Konsekuensi hukum atas perbuatan tersebut adalah pidana penjara paling dan/atau denda sesuai dengan ketentuan pasal tersebut.

Adapun pasal 45 Ayat (4), "Setiap orang yang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan menuduhkan suatu hal untuk diketahui umum dalam bentuk informasi elektronik dan/atau dokumen elektronik dapat dipidana penjara maksimal 2 tahun dan/atau denda maksimal Rp 400 juta." Dalam konteks penyalahgunaan deepfake pornografi, pelaku yang melakukan penghinaan dapat dijerat dengan hukum, Yang mana perbuatan tersebut dilakukan dengan niat jahat dan tanpa izin, dan melibatkan distribusi, transmisi, atau pembuatan informasi elektronik dan/atau dokumen elektronik yang dapat diakses oleh publik.

Selanjutnya, pasal 51 Ayat (1) "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. Tindakan ini diancam dengan hukuman pidana dengan penjara paling lama 12 tahun atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)."

4. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Sejalan dengan teori pertanggungjawaban pidana yang diuraikan sebelumnya, penulis menemukan bahwa dalam UU PDP, seseorang dapat dikenai pertanggungjawaban pidana karena melanggar ketentuan dalam Pasal 65 ayat (1), (2), (3), dan Pasal 66 dengan kesengajaan. Adapun dalam pasal 68 "Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana

¹⁸ Hukum Online, Catatan Pidana Alternatif dalam RKUHP, dalam <https://www.hukumonline.com/berita/a/catatan-pidana-alternatif-dalam-rkuhp-lt5af575fd904a>, Diakses pada 11 Mei 2018.

dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000. 000.000,00 (enam miliar rupiah).”

Pasal 69 menyatakan, "selain dijatuhi pidana sesuai Pasal 67 dan Pasal 68, pelaku juga dapat dikenai pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari tindak pidana serta pembayaran ganti kerugian." UU PDP menerapkan model sanksi pidana kumulatif, di mana pidana penjara dan denda merupakan sanksi pokok, dan pengambilalihan harta benda atau keuntungan hasil kejahatan serta pembayaran ganti rugi merupakan sanksi tambahan. Pasal 12 UU PDP menjamin hak subjek data pribadi atau korban untuk menuntut dan memperoleh ganti rugi atas pelanggaran terkait data pribadi dengan ketentuan yang berlaku. Dengan demikian, penyalahgunaan deepfake tergolong sebagai delik aduan.

Berdasarkan kajian pustaka, pertanggungjawaban pidana dapat diartikan sebagai proses penentuan apakah seseorang dapat dimintai pertanggungjawaban atas tindak pidana yang diperbuat dan menerima hukuman dari pengadilan. Yang berarti pertanggungjawaban pidana menentukan apakah seseorang akan diberikan kebebasan atau dijatuhi hukuman. Dalam konteks kejahatan dunia maya, pelaku memiliki kewajiban hukum untuk bertanggung jawab atas kerugian yang mereka sebabkan. Pelaksanaan hak dan kewajiban hukum selalu memerlukan adanya pertanggungjawaban hukum. Hans Kelsen juga berpendapat bahwa kewajiban hukum dan pertanggungjawabannya merupakan hal yang saling berkaitan. Dengan demikian, seseorang memiliki kewajiban untuk bertanggung jawab secara hukum atas perbuatan tertentu, yang berarti dia harus menanggung akibat dari perbuatannya. Teknologi deepfake tidak hanya menimbulkan tantangan dalam pengaturan hukum, tetapi juga dalam hal pertanggungjawaban hukum terhadap pelaku.

Terkait penyalahgunaan deepfake, termasuk dalam kategori perbuatan yang dapat dianggap sebagai tindak pidana. Seseorang dianggap melakukan perbuatan pidana jika perbuatannya terbukti melanggar ketentuan hukum pidana yang berlaku. Syarat kriminalisasi penyalahgunaan deepfake telah terpenuhi, baik dari segi subjektif maupun objektif. Penggunaan deepfake secara tidak bertanggung jawab, yang berpotensi menimbulkan kerugian bagi orang lain adalah perbuatan yang tidak dibenarkan dan melanggar hukum, karena hasilnya bertentangan dengan hukum serta menimbulkan kerugian bagi orang lain. Penyebaran konten yang dihasilkan dari penyalahgunaan deepfake juga dapat dianggap sebagai penyalahgunaan,

kecuali jika penggunaan teknologi tersebut hanya untuk keperluan pribadi tanpa merugikan orang lain.

Di Indonesia, pelaku penyalahgunaan deepfake pornografi dapat dijerat dengan berbagai ketentuan hukum yang sudah ada, seperti UU ITE, UU Pornografi, dan UU Perlindungan Data Pribadi. Namun, pengaturan hukum yang ada belum secara eksplisit mencakup kasus-kasus yang melibatkan teknologi manipulasi seperti deepfake.¹⁹ Ketiadaan undang-undang khusus mengharuskan penegak hukum menggunakan pengaturan umum terkait pencemaran nama baik, informasi elektronik, pornografi, dan perlindungan data pribadi untuk menangani tindak pidana seperti deepfake pornografi yang disebarluaskan melalui internet. Sistem hukum positif di Indonesia dapat menjadi dasar hukum untuk mengatur sanksi bagi pelaku penyalahgunaan teknologi deepfake. UU ITE berfungsi sebagai *lex specialis* yang mengatur kejahatan di dunia maya secara lebih rinci, di mana Pasal 27 ayat (1) melarang distribusi informasi yang bertentangan dengan kesusilaan dan Pasal 45 mengatur sanksi pidana bagi pelanggarnya. Selain itu, UU Pornografi Pasal 4 ayat (1) melarang produksi dan penyebaran konten pornografi. Namun, pengaturan ini masih belum mampu mengakomodasi kompleksitas kejahatan yang melibatkan deepfake.

Berdasarkan teori pertanggungjawaban pidana, pertanggungjawaban selalu terkait dengan unsur *mens rea* yang hanya dimiliki manusia. Kecerdasan buatan tidak memiliki *mens rea*, karena kemampuan berpikirnya merupakan hasil pemikiran manusia yang dikemas dalam sistem komputer dan algoritma. Pertanggungjawaban pidana bersifat personal dan tidak dapat dialihkan, sehingga subjek hukum yang harus bertanggung jawab atas pencemaran nama baik akibat penggunaan deepfake adalah pembuat video tersebut. Untuk dapat bertanggung jawab, seseorang harus mampu membedakan antara perbuatan baik dan buruk sesuai hukum (faktor akal) serta menentukan kehendaknya berdasarkan penilaian tersebut (faktor kehendak). Sanksi pidana dapat dijatuhkan setelah seseorang melakukan tindak pidana dan dimintai pertanggungjawaban, yang kemudian menentukan jenis, berat, dan lamanya pidana yang dijatuhkan.

Dari keseluruhan pemahaman diatas maka dapat ditarik suatu pemahaman bahwa AI berperan sebagai objek hukum di Indonesia dan tidak dapat didefinisikan sebagai subjek hukum. Manusia adalah aktor yang bertanggung jawab atas pengoperasian AI, sehingga dalam

¹⁹ Indah Rohmawati, Amir Junaidi & Ariy Khaerudin, *Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)*, Journal Of Social Science Research, Vol. 4 No. 6, 2024

hukum positif, manusia berperan sebagai subjek. Tanggung jawab penggunaan AI sepenuhnya ada pada penyelenggara, kecuali dalam keadaan darurat yang dapat membebaskan tanggung jawab tersebut. Meskipun AI memiliki kemampuan luar biasa dalam menganalisis data, kemampuan ini bergantung pada instruksi dari pengguna manusia. Oleh karena itu, tanggung jawab pada penggunaan teknologi ini secara bijaksana sepenuhnya berada di tangan manusia sebagai pengambil keputusan, agar AI digunakan untuk tujuan positif dan tidak merugikan orang lain.

Fenomena deepfake pornografi menunjukkan betapa pentingnya hukum untuk dapat mengikuti perkembangan teknologi. Tanpa pembaruan, hukum akan terus tertinggal dalam menangani kejahatan digital yang semakin kompleks. Di Indonesia, regulasi yang ada, meskipun relevan dalam beberapa aspek, masih bersifat umum dan tidak secara eksplisit mencakup teknologi deepfake. Akibatnya, proses penanganan kasus sering terhambat oleh kurangnya perangkat hukum yang spesifik.

Dari keseluruhan pemahaman dapat di atas diambil kesimpulan bahwa terhadap pelaku penyebaran deepfake pornografi, pelaku bertanggung jawab atas konsekuensi dari perbuatan yang merugikan. Bahwa pelaku yang memanipulasi menggunakan deepfake yang mencemarkan nama baik seseorang dapat dipidana menurut pasal pencemaran baik dalam KUHP. Demikian juga pertanggungjawaban atas tindakan yang menyebarkan informasi elektronik bersifat pornografi merupakan perbuatan pidana Informasi elektronik yang disebarkan melanggar kesusilaan dan bersifat pornografi sehingga melanggar ketentuan Pasal 27 ayat (1) dan Pasal 4 ayat (1) juncto Pasal 29 UU Pornografi.

KESIMPULAN

Penggunaan *Artificial Intelligence* (AI) memberikan berbagai manfaat penting. Namun, penerapan AI juga datang dengan risiko, terutama penyalahgunaan teknologi *deepfake* sebagai bagian dari AI. Penerapan hukum pidana terhadap perbuatan penerapan penyimpangan AI telah sesuai dengan ketentuan yang berlaku, meskipun belum secara eksplisit disebutkan dalam peraturan terkait. Akan tetapi, peraturan yang ada telah menyediakan dasar hukum untuk menjerat pelaku. Meskipun belum sepenuhnya mampu mengakomodasi kompleksitas tindak pidana yang ditimbulkan oleh teknologi *deepfake*. Terdapat kekosongan hukum dan masih memerlukan penguatan lebih lanjut, tanpa pengelolaan yang tepat, risiko penyalahgunaan terhadap data pribadi dapat menjadi ancaman serius. Pertanggungjawaban pidana atas

penyalahgunaan *deepfake* oleh pelaku didasarkan pada bentuk tindak pidana yang dilakukannya. Regulasi yang berlaku di Indonesia saat ini dapat dijadikan dasar hukum yang mengatur sanksi bagi tindak pidana kepada para pelaku penyalahgunaan teknologi *deepfake* pornografi yang dapat dikenakan meliputi pidana penjara dan denda. Pertanggungjawaban pidana dapat dikenakan pada seseorang apabila terbukti secara sengaja dan melawan hukum dengan sengaja dan tanpa hak menyebarluaskan konten yang bermuatan asusila. Namun, pembuktian dalam proses pertanggungjawaban pidana bagi pelaku lebih kompleks karna masih belum ada peraturan yang dengan spesifik menjelaskan terkait teknologi AI khususnya dibidang kekerasan seksual berbasis elektronik AI.

DAFTAR PUSTAKA

- Astuti, P., & Novyanti, H. (2022). Jerat Hukum Penyalahgunaan Aplikasi *Deepfake* Ditinjau Dari Hukum Pidana. *Novum: Jurnal Hukum*. 9 (4).
- Awawangi, R.V. Pencemaran Nama Baik Dalam KUHP Dan Menurut UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Lex Crimen*. 3 (4).
- Bayu, P., Fikri, A., Viqran, M. (2023). [*Recontruction Of Personal Data Protection Law Againts Data Leakage In The Digitalization Era After The Covid-19 Pandemic*](#). *Lembuswana Law Review: Public Law, Civil Law, Business Law*. 1 (1).
- Damarjati. (2019). Fenomena *Deepfake* dan Tantangan Hukum Siber di Indonesia, *Jurnal Hukum dan Teknologi Informasi*. 5 (1).
- Databoks. (2024, Januari 31). Indonesia Penyumbang Kunjungan Aplikasi AI Terbanyak ke-3 diDunia.
<https://databoks.katadata.co.id/teknologitelekomunikasi/statistik/a49ed3eb121983b/indonesia-penyumbang-kunjungan-ai-terbanyak-ke-3-di-dunia>.
- Galih, D., & Ramadhan. (2022). Perlindungan Hukum Atas Invensi Artificial Intelligence Di Era Revolusi Industri 4.0 & Society 5.0. Universitas Islam Indonesia.
- Hidayat, N. (2017). Rujukan Dan Aplikasi Sistem Hukum Indonesia Berdasarkan Pasal 1 Ayat (3) UUD 1945 Pasca Amandemen Ke Tiga. *Uir Law Review*. 1 (2).
- Huda, C. (2006). Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan. Jakarta: Kencana.

- Hukum Online. (2018, Mei 11). Catatan Pidana Alternatif dalam RKUHP. <https://www.hukumonline.com/berita/a/catatan-pidana-alternatif-dalam-rkuhp-lt5af575fd904a>.
- Kansil, C., & Christine, B. (2022). Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Syntax Literate: Jurnal Ilmiah Indonesia*. 7 (9).
- Karo, R. K., & Laza, J. M. (2023). Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan *Deepfake* Technology Pada Perspektif UU PDP dan GDPR. *Lex Prospicit*. 1 (2).
- Khaerudin, A., Junaidi A., & Rohmawati. (2024). Urgensi Regulasi Penyalahgunaan *Deepfake* Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO). *Journal Of Social Science Research*. 4 (6).
- Laughlin, K.S. Westin: Privacy and Freedom Westin: Privacy and Freedom Recommended Citation Recommended Citation. *Michigan Law Review*. 66
- Mahkamah Konstitusi Republik Indonesia. (2024, Januari 31). DPR: Ketentuan Pidana dalam UU ITE Diatur dalam KUHP Nasional, dalam <https://www.mkri.id/index.php?page=web.Berita&id=19637>.
- Maulana, R., & Mutiara, U. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*. 1 (1).
- Oratmangun, Y.A. (2016). Kajian Hukum Terhadap Kemampuan Bertanggung Jawab Menurut Pasal 44 KUHP. *Lex et Societatis*. 4 (5).
- Rahayu, R. A., & H. S. (2023). Analisis Gambar Wajah Palsu: Mendeteksi Keaslian Gambar Yang Dimanipulasi Menggunakan Metode Variational Autoencoder Dan Forensics Deep Neural Network, *Sibatik Jurnal*. 2 (9).
- Rongkene, B. (2020). Tindak Pidana Pornografi Menurut KUHP Dan Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi. *Lex Crimen*. 9 (1).
- Sujamawardi, H. (2018). Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Dialogia Iuridica Jurnal Hukum Bisnis dan Investasi*. 9 (2).

Sumanto, L,. & Angelina, J. (2025). Kajian Yuridis Kasus Pencemaran Nama Baik Berdasarkan KUHP yang Berkepastian Hukum. *Journal of Accounting Law Communication and Technology*. 2 (1).

Tim Departemen Pendidikan Nasional, 2005, Kamus Besar Bahasa Indonesia, Pusat Bahasa Departemen Pendidikan Nasional, Balai Pustaka, Jakarta, hal.1139.

Young, N. *DeepFake* Technology: Complete Guide to *Deepfakes*, Politics and Social Media