CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Perlindungan Hukum Terhadap Korban Penyalahgunaan Deepfake Dalam Pornografi

Khairunnisa Maharani

Email: khairunnisa21002@mail.unpad.ac.id

Universitas Padjadjaran

Abstrak

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) telah memunculkan bentuk kejahatan baru berupa deepfake pornografi, yaitu pembuatan konten pornografi non-konsensual dengan memanipulasi data pribadi seseorang tanpa persetujuan. Praktik ini menimbulkan pelanggaran serius terhadap hak privasi, kehormatan, dan perlindungan data pribadi korban. Penelitian ini bertujuan untuk menganalisis peranan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam melindungi hak korban deepfake pornografi di Indonesia serta membandingkannya dengan pengaturan deepfake di China. Hasil penelitian menunjukkan bahwa UU PDP telah memberikan dasar perlindungan hukum terhadap pemrosesan data pribadi tanpa persetujuan, namun pengaturannya masih bersifat umum dan belum secara khusus mengatur penyalahgunaan teknologi AI dalam deepfake pornografi. Oleh karena itu, diperlukan penguatan regulasi dan pengawasan untuk memberikan perlindungan hukum yang lebih efektif bagi korban.

Kata kunci: Deepfake, Pornografi, Perlindungan Data Pribadi, UU PDP

Article History
Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Copyright : Author
Publish by : CAUSA

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pun mengubah perilaku masyarakat dan peradaban global. Dimana, perkembangannya menjadikan dunia menjadi tanpa batas (borderless) dan perubahan sosial yang secara signifikan berlangsung sangat cepat[1]. Di era digital, terlihat bahwa teknologi dan internet sangat memudahkan pekerjaan manusia. Salah satu buktinya dapat dilihat dari banyaknya aplikasi perpesanan dan telekonferensi untuk menunjang pekerjaan dan pembelajaran jarak jauh. Saat ini, Artificial Intelligence (AI) atau kecerdasan buatan sedang ramai diperbincangkan sebagai salah satu bukti perkembangan ilmu pengetahuan dan teknologi yang melebihi ekspektasi manusia. Bahkan, banyak instansi atau perorangan yang berlomba-lomba menciptakan atau mengembangkan Al.

[1] Ahmad M. Ramli, Cyber Law dan HAKI Dalam Sistem Hukum Indonesia, Bandung: Refika Aditama, 2004, hlm. 1.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Kecerdasan manusia dalam menciptakan Al terkadang membuat kecanggihan Al di luar kendali manusia, apalagi kecerdasan manusia yang semakin berkembang membuat manusia semakin curang sehingga dapat membuat ancaman besar bagi dunia. Dalam perkembangan teknologi, banyak kejahatan berbasis digital yang terjadi seperti serangan digital berupa Cyberbullying atau Pemerasan dan Kekerasan Berbasis Gender Online (KBGO). Di era kemajuan ilmu pengetahuan dan teknologi saat ini, teknologi dan ilmu pengetahuan juga berkembang dengan pesat, oleh karena itu, semakin berkembang pula bidang kejahatan dan pelanggaran hukum. Kejahatan pornografi semakin berkembang dari waktu ke waktu, salah satunya adalah hadirnya pornografi non-konsensual, yang terbagi menjadi pornografi balas dendam dan deep fakes (pornografi palsu). Pornografi palsu adalah tindakan mempublikasikan gambar atau konten seksual eksplisit dari seseorang dalam bentuk foto atau video tanpa persetujuannya, yang dapat dibuat dengan menggunakan aspek kecerdasan buatan (seperti kecerdasan buatan) atau tanpa menggunakan aspek tersebut[2].

Kedua jenis pornografi ini serupa karena keduanya bertujuan untuk membalas dendam pelaku terhadap korban, tetapi perbedaannya terletak pada keaslian konten seksualnya. Revenge porn bisa didapatkan dari foto atau video asli korban, sedangkan deep fakes adalah foto atau video buatan yang didapatkan dari rekaman yang sudah tersebar di publik, kemudian diolah dengan kecerdasan buatan (Al). Deep fakes dapat dibuat dengan menggunakan beberapa aplikasi dengan teknologi pengenalan wajah untuk mencocokkan artis porno yang mirip dengan orang yang ingin ditukar wajahnya oleh pelaku[3].

Meskipun sudah ada beberapa peraturan perundang-undangan yang menjadi payung hukum untuk menindak pelaku penyebar konten pornografi, namun menurut penulis, UU dan peraturan tersebut belum cukup untuk melindungi data pribadi korban. Pelaku masih bisa ditindak, namun data pribadi korban masih bisa diakses secara bebas oleh publik. Bahkan, undang-undang dan peraturan yang disebutkan di atas juga tidak memadai untuk menghukum pembuat konten pornografi palsu atau buatan, yang tidak hanya menyebarkan, tetapi juga membuat konten dengan menyalahgunakan Al.

Penggunaan Al dalam deep fakes tidak hanya melanggar privasi korban, tetapi juga melibatkan pelanggaran data pribadi karena menggunakan foto atau video pribadi seseorang tanpa izin. Oleh karena itu, deep fakes jelas melanggar hak privasi dan kehormatan seseorang. Dari sudut pandang yurisdiksi, deep fakes sudah dianggap sebagai tindakan ilegal

[2] Mesra Betty Yel and Mahyuddin K. M. Nasution, "Information Security of Personal Data on Social Media", Jurnal Informatika Kaputama (JIK), Vol. 6 No. 1 (January 2022), pp. 98.
[3] Ananthia Ayu, Titis Anindyajati, and Abdul Ghoffar, "Protection of the Right to Privacy over Personal Data in the Digital Economy Era", Research Results in the Registrar and Secretariat General of the Constitutional Court, (2019). p. 97

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

dan melanggar hukum privasi dan kehormatan seseorang dalam hal norma-norma sosial. Hingga saat ini, belum ada undang-undang yang secara khusus mengatur penggunaan AI dalam deep fakes. Meskipun ada UU ITE dan UU Pornografi, namun kedua UU tersebut hanya berfokus pada penyebar konten pornografi, bukan pada hak-hak korban, seperti data pribadi. Hal ini tentu mengancam data pribadi seseorang berupa foto atau video yang menandakan identitas orang tersebut. Belum lagi, jika pembuat konten yang memalsukan tersebut juga mencantumkan nama, alamat, dan hal-hal penting lainnya dari orang yang menjadi objek video tersebut. Perlindungan data pribadi harus ditegakkan untuk mencegah penyalahgunaan AI dalam kasus-kasus seperti deep fakes. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memadai dan kesadaran akan konsekuensi hukum dapat membantu melindungi individu dari eksploitasi seperti deep fakes dan KBGO. Selain itu, kampanye kesadaran tentang konsekuensi negatif dari deep fakes dengan penggunaan AI perlu dilakukan untuk mencegah lebih banyak kasus revenge porn dan deep fakes di masa depan.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan perbandingan hukum. Pendekatan perundang-undangan dilakukan melalui analisis terhadap UU Perlindungan Data Pribadi, UU ITE, dan UU Pornografi. Pendekatan perbandingan hukum digunakan dengan mengkaji pengaturan deepfake di China sebagai bahan evaluasi bagi pengembangan hukum di Indonesia. Bahan hukum yang digunakan meliputi bahan hukum primer dan sekunder.

PEMBAHASAN

1. Peranan Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam melindungi hak korban *deepfakes* pornografi di Indonesia

Data akan dianggap sebagai data pribadi jika memungkinkan untuk mengidentifikasi seseorang dalam data tersebut[4]. Data pribadi penting karena dapat digunakan untuk mengidentifikasi seseorang untuk membantu proses yang tidak melanggar hukum. Hal ini perlu dipahami sebagai akibat dari penggunaan data pribadi yang telah melewati batas-batasnya seperti digunakan dalam tindakan ilegal pencurian identitas. Setiap warga negara memiliki kewajiban dan hak untuk melindungi data pribadi mereka sendiri.

[4]Shigenori Matsui, "The Criminalisation of Revenge Porn in Japan", Washington International Law Journal Association, Vol. 24, No. 2, pp. 289

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Setiap warga negara memiliki kewajiban dan hak untuk melindungi data pribadinya. Data pribadi adalah data yang kepemilikannya hanya akan diketahui dan dapat diproses oleh setiap pemiliknya secara individual yang melekat pada pemilik tersebut[5].

Setiap identitas pribadi merupakan bentuk data pribadi, tidak terkecuali adanya pemalsuan. Deep fakes merupakan salah satu bentuk manipulasi dalam dunia media digital yang mana identifikasi akan sangat sulit dibedakan dengan bentuk data aslinya. Munculnya deep fakes merupakan bencana dalam penggunaan media sosial saat ini. Sifat media sosial yang sangat terbuka memang menjadi salah satu bentuk kebebasan dalam mengekspresikan diri. Namun, tentu saja dalam setiap tindakan yang terlalu bebas, akan ada celah yang dapat menimbulkan kerugian. Para pemalsu dengan gaya manipulasinya seakan-akan dapat mengubah identitas seseorang dengan menggunakan teknologi untuk mengubah data pribadi menjadi identitas baru. Perubahan identitas ini jika dilihat dalam tindakan deep fakes akan membuat ancaman dari pemilik identitas asli karena seperti yang terjadi, perubahan identitas ini menjadi tidak senonoh dan berbau seksual. Melalui Al, identitas dapat dibuat menjadi identitas baru dengan menggunakan teknologi algoritma visualisasi. Teknologi ini bekerja dengan cara membuat kecocokan baru pada sebuah identitas, kemudian memasangkannya dan mengubah identitas tersebut menjadi data baru yang terlihat seolah-olah seperti identitas aslinya. Pemalsuan mendalam terjadi ketika identitas asli telah menjadi data baru yang meyakinkan secara visual. Para pelaku deep fakes dapat melakukan hal ini dengan mudah dan bebas, yang mengakibatkan kehancuran reputasi dan bahkan pencemaran nama baik bagi para korbannya. Korban pemalsuan mendalam akan mengalami kerugian yang sangat besar jika identitas mereka digunakan untuk membuat pemalsuan mendalam pornografi. Terlepas dari manipulasi, tampilan wajah korban yang memalukan dan jelas-jelas berbahaya. Korban merasa bahwa kejahatan telah dilakukan terhadapnya, yang mengakibatkan pencemaran nama baik atau identitas korban.

Melihat perkembangan teknologi yang begitu cepat, sangat disayangkan jika hukum tidak selalu dapat mengikuti perubahan dan ancaman baru yang berpotensi muncul. Oleh karena itu, jika melihat hukum positif di Indonesia, ketentuan mengenai Al belum diatur secara khusus namun ketentuan tersebut dapat diperoleh dari penafsiran hukum atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Sejauh ini, Al 1 diakui oleh rezim hukum hak cipta sebagai karya berhak cipta dari pencipta dan diakui oleh rezim hukum paten sebagai penemuan. Terlepas dari kecerdasan

[5] Shigenori Matsui, Ibid, p. 291

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

buatan, tindakan Al yang bergerak secara sepihak dapat menimbulkan hak dan kewajiban. Pasal 1367 KUH Perdata menyatakan bahwa "Seseorang bertanggung jawab tidak saja untuk kerugian yang disebabkan karena perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan karena perbuatan orang-orang yang menjadi tanggungannya atau karena barang-barang yang berada di bawah pengawasannya". Dari pasal tersebut, dapat disimpulkan bahwa pemilik Al tidak hanya bertanggung jawab atas perbuatannya sendiri, tetapi juga atas kerugian dan barang yang berada di bawah pengawasannya. Selain itu, Pasal 27 UU ITE melarang pendistribusian atau pembuatan informasi elektronik yang memiliki muatan pelanggaran asusila (pornografi). Selain itu, pembuatan dan penyebaran deep fakes dapat dikategorikan sebagai pencemaran nama baik karena dalam deep fakes terdapat identitas seseorang yang dimanipulasi, sehingga dapat disimpulkan bahwa pemilik Al serta pembuat dan penyebar konten deep fakes dapat dimintai pertanggungjawaban.

Dalam konteks UU Perlindungan Data Pribadi, deep fakes dapat dikatakan sebagai data pribadi karena memenuhi kriteria yang dijelaskan dalam Pasal 1 angka 1 UU PDP bahwa:

> *"Data pribadi adalah data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara perseorangan atau yang dapat dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.*

Menurut penulis, deep fakes termasuk dalam salah satu kategori data pribadi karena hasil dari deep fakes tetap mengidentifikasi atau menunjukkan profil seseorang secara individual maupun kombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau sistem non elektronik meskipun hasil tersebut diperoleh dari proses manipulasi atau rekayasa.

Konsep dasar pemahaman mengenai larangan menggunakan data orang lain telah telah diatur dalam Pasal 65 UU PDP Ayat 1 bahwa:

> *“Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.”*

Jika kita telusuri tindakan pelaku, proses pembuatan deep fakes dengan cara mengambil foto seseorang dari media sosial tanpa izin dan memanipulasinya untuk kepentingan pribadi, telah menunjukkan bahwa data pribadi tersebut bukan milik si pembuat deep fakes dan data pribadi tersebut diperoleh secara melawan hukum tanpa persetujuan pemilik asli yang identitasnya dimanipulasi. Konten deep fakes tentu saja merugikan pihak-pihak tertentu, larangan serupa juga tertulis dalam Pasal 66 UU PDP." Korban dari fenomena deep fakes sebagai pemilik data pribadi berupa foto atau video disebut sebagai Subjek Data Pribadi. Berdasarkan Pasal 1 angka 6 UU PDP, subjek data pribadi adalah orang perseorangan yang

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

data pribadinya dilekatkan. Sebagai subjek data pribadi, korban memiliki hak atas data pribadinya. Hak-hak subjek data pribadi tercantum dalam Pasal 5 sampai dengan Pasal 15 UU PDP.

Proses pembuatan pemalsuan mendalam terjadi dengan ketidaktahuan korban, bahkan tanpa bahkan tanpa persetujuan korban. Oleh karena itu, dalam konteks ini, tidak ada kesepakatan atau persetujuan, yang mengakibatkan pelanggaran pemrosesan data pribadi. Sebelum kita membahas persetujuan dalam pemrosesan data pribadi pribadi, ruang lingkup pengolahan data pribadi itu sendiri terdiri dari akuisisi dan pengumpulan; pemrosesan dan analisis; penyimpanan; koreksi dan pembaruan; tampilan, pengumuman, pemindahan, penyebarluasan, atau pengungkapan; dan/atau penghapusan atau pemusnahan. Pemrosesan data pribadi dikendalikan oleh Pengendali Data Pribadi. Pasal 20 ayat (1) UU PDP menegaskan bahwa Pengontrol Data Pribadi harus memiliki dasar untuk memproses Data Pribadi. Pengontrol Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak secara sendiri-sendiri atau bersama-sama dalam menentukan menentukan tujuan dan menjalankan kendali atas pemrosesan Data Pribadi. Dalam konteks pemalsuan palsu, Pengontrol Data Pribadi adalah pembuat konten palsu yang memiliki korban yang memiliki data pribadi yang bersifat publik, misalnya foto atau video. Pengontrol Data Pribadi memiliki kewajiban yang terdapat pada Pasal 20 ayat (1) dan (2) UU PDP. Ayat (2) menyatakan alasan pemrosesan data pribadi, salah satunya adalah persetujuan hukum yang eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau lebih tujuan tertentu yang telah disampaikan oleh Pengontrol Data Pribadi kepada Subjek Data Pribadi.

Melihat Pasal 20 UU PDP, dapat disimpulkan bahwa pembuatan konten deep fakes bukan merupakan pengolahan data pribadi karena tidak pernah mendapatkan persetujuan hukum secara eksplisit dari Subjek Data Pribadi. Oleh karena itu, korban sebagai subjek data pribadi memiliki hak untuk meminta agar pemrosesan tersebut dihapus.'" Namun, penjagaan terhadap hak-hak subjek data pribadi tidak dikawal dengan pengawasan yang baik, sehingga masih banyak konten-konten deep fakes yang beredar di luar sana. Dapat dinilai bahwa peran UU PDP dalam melindungi data pribadi korban deep fakes sebenarnya belum mencukupi kebutuhan korban. Terlebih lagi, tidak ada sanksi yang rinci bagi para pembuat konten pornografi palsu yang menggunakan bantuan kecerdasan buatan (artificial intelligence/AI) dalam peraturan perundang-undangan di Indonesia, khususnya UU ITE dan UU Pornografi. Bahkan dalam UU ITE, sanksi hanya diatur untuk penyebar atau penyebar konten yang mengandung unsur asusila.

2. Pengaturan mengenai mengenai Deepfake di China

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

China selangkah lebih maju dibandingkan dengan indonesia. Pengaturan mengenai deepfake di China telah menjadi lebih ketat, dengan Cyberspace Administration of China (CAC) merilis aturan yang mewajibkan perusahaan teknologi memverifikasi identitas pengguna sebelum menggunakan teknologi deepfake dan kecerdasan buatan (AI). Aturan ini bertujuan untuk mengatur teknologi yang menghasilkan atau memanipulasi teks, gambar, audio, atau video menggunakan deepfake, serta memastikan bahwa perusahaan tidak menggunakan deepfake untuk tujuan ilegal seperti penipuan, skema, atau penyebaran informasi palsu yang berbahaya.

CAC mendeskripsikan teknologi sintesis mendalam sebagai teknologi yang menggunakan pembelajaran mendalam, realitas virtual, dan algoritme sintetis lainnya untuk menghasilkan teks, gambar, audio, video, adegan virtual, dan informasi jaringan lainnya. Ini termasuk, namun tidak terbatas pada:[6]

a. Teknik untuk membuat atau mengubah teks
b. Teknologi untuk membuat atau mengubah konten suara, seperti konversi teks ke suara dan atribut suara
c. Teknik untuk membuat atau mengubah konten non-suara, seperti musik
d. Teknik untuk membuat atau mengubah fitur biometrik dalam gambar dan konten video, seperti pembuatan wajah, penggantian wajah, atau manipulasi gerakan
e. Rekonstruksi 3D, simulasi digital, dan teknologi lain yang membuat atau mengubah model 3D

Selain itu, China juga memiliki pengaturan bernama Rule on Deepfake of Internet Information Services (RDIIS). Pengaturan deepfake ini bertujuan untuk mengatur layanan informasi internet yang berbasis teknologi deepfake. Teknologi deepfake tentu saja memperluas pengalaman pengguna, tetapi pada saat yang sama berita dan informasi palsu, bahkan kecurangan dapat dilakukan dengan mudah dilakukan dengan menggunakan teknologi deepfake. Oleh karena itu, pemberitahuan penggunaan teknologi deepfake terlalu penting. Pertama, penyedia layanan deepfake berkewajiban untuk menandai secara jelas informasi yang dihasilkan atau informasi yang diedit di lokasi dan area yang wajar, untuk mengingatkan publik tentang keadaan deepfake jika layanan deepfake dapat menyebabkan kebingungan atau Peraturan Kecerdasan Buatan di Tiongkok 683 kesalahpahaman oleh publik. Kedua, penyedia layanan dan pendukung teknis harus secara eksplisit memberi tahu pengguna untuk menandai konten deepfake dan mendapatkan persetujuan dari individu yang informasi

[6] China Briefing, https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ , diakses pada 27 Juni 2024

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

biometriknya digunakan. Selain itu, mereka harus mengotentikasi informasi identitas asli pengguna melalui nomor ponsel mereka, nomor ID atau kode kredit sosial terpadu atau identifikasi jaringan nasional publik layanan publik, dan tidak akan memberikan layanan penerbitan informasi kepada pengguna yang belum yang belum mengautentikasi informasi identitas asli mereka.

Penyedia layanan dan pendukung teknis harus secara independen melakukan penilaian keamanan atau memberi wewenang kepada lembaga profesional untuk melakukannya sesuai dengan hukum, jika alat yang mereka sediakan memiliki fungsi untuk menghasilkan atau mengedit informasi biometrik pada wajah dan suara manusia, atau menghasilkan, mengedit informasi non-biometrik pada objek dan adegan khusus yang mungkin melibatkan keamanan nasional, citra nasional, kepentingan nasional, dan kepentingan publik. Namun, penilaian keamanan harus dilakukan sesuai dengan dokumen resmi terkait jika penyedia layanan mengembangkan dan meluncurkan produk, aplikasi, dan fungsi baru dengan atribut opini publik atau kemampuan mobilisasi sosial. Sebagaimana persyaratan perekaman yang diatur dalam RARIIS, penyedia layanan dan pendukung teknis juga harus melakukan perekaman kepada pihak yang berwenang, jika layanan deepfake tersebut berkaitan dengan opini publik dan mobilisasi sosial, yang menariknya sesuai dengan ketentuan RARIIS, yang berarti mereka juga harus melakukan perekaman dalam waktu sepuluh hari setelah layanan dimulai. Sebenarnya, RDIIS berfokus pada kewajiban hukum bagi penyedia layanan dan pendukung teknis. Kewajiban hukum bagi pengguna adalah bahwa mereka tidak boleh memproduksi, menyalin, mempublikasikan, atau menyebarkan informasi berita palsu dan mendapatkan layanan deepfake dengan informasi identitas asli, dan menjaga informasi mereka sendiri tetap benar[7].

KESIMPULAN

Di dunia yang serba digital seperti sekarang ini, penting bagi setiap pemilik identitas untuk memahami pentingnya data pribadi mereka. Bagaimanapun juga, korban pemalsuan identitas pada dasarnya harus memastikan bahwa data pribadi mereka akan aman dan tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Data pribadi harus dijaga sebaik kita menjaga data yang sangat rahasia.

Data pribadi telah diatur dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menekankan pada perlindungan dan penegakan hukum terhadap perbuatan yang melanggar penggunaan data pribadi secara umum dan luas. Jika dilihat dari permasalahan

[7] Qingle Hu , Wei Liu, The Regulation of Artificial Intelligence in China.

Jurnal Hukum dan Kewarganegaraan
Vol 16 No 2 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

pemalsuan dalam, peran UU PDP telah mengakomodir hak korban untuk melindungi data pribadinya serta larangan penyebarluasan data pribadi dan tindakan pemalsuan data pribadi. Namun, peran UU PDP masih bersifat umum dan belum dikawal dengan pengawasan yang baik, sehingga konten-konten palsu masih banyak tersebar di berbagai platform dan belum bisa ditangani secara maksimal. Selain itu, tidak ada sanksi yang rinci bagi pembuat konten pornografi palsu yang menggunakan kecerdasan buatan (artificial intelligence/AI) dalam peraturan perundang-undangan di Indonesia, terutama dalam UU ITE dan UU Pornografi, meskipun UU ITE hanya mengatur sanksi bagi penyebar atau penyebar konten yang mengandung unsur asusila.

DAFTAR PUSTAKA

Perundang-Undangan

Udang-Undang Nomor 44 Tahun 2008 Tentang Pornografi

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Buku

Dikdik M.Arief Mansur dan Elisatris Gultom, Cyber Law: Aspek Hukum Teknologi Informasi, Bandung: Refika Aditama, 2005.

Muhamad Amirulloh, Hukum Teknologi, Informasi dan Komunikasi Sebagai Hukum Positif di Indonesia Dalam Perkembangan Masyarakat Global, Bandung: Unpad Press, 2016,

Ahmad M. Ramli, Cyber Law dan HAKI Dalam Sistem Hukum Indonesia, Bandung: Refika Aditama, 2004.

Jurnal

Alcianno G.Gani, “Cybercrime (Kejahatan Berbasis Komputer)”, JSI (Jurnal Sistem Informasi), Vol.5 No.1, 2018.

Fiorida Mathilda, “Cybercrime Dalam Sistem Hukum Indonesia”, Sigma-Mu Vol.4 No.2, 2012, hlm. 2012

Anggia Dasa Putri dan Dapit Pratama, “Sistem Pakar Mendeteksi Tindak Pidana Cybercrime Menggunakan metode Forward Chaining Berbasis Web di Kota Batam”, Jurnal Edik Informatika, Vol. 3 No. 2, Maret 2017.

Lia Sautunnida, “Urgensi Undang-undang Pelindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia”, Kanun Jurnal Ilmu Hukum, Volume 20, Nomor 2, 2018.

Ririen Kusumawati, “Kecerdasan Buatan Manusia (Artifcial Intelligence): Teknologi Impian Masa Depan”, Jurnal Ulul Albab: Jurnal Studi Islam, Vol. 9, No. 2, 2008.

Qingle Hu , Wei Liu, The Regulation of Artificial Intelligence in China.