JURNAL SPEKTRUM HUKUM
Volume 21 No 2 Oktober 2024
ISSN Print: 1858-0246 | ISSN Online: 2355-1550
DOI : 10.56444/sh
http://jurnal.untagsmg.ac.id/index.php/sh

Ancaman Deepfake Buatan AI Dan Implikasinya Terhadap Keamanan Data Biometrik Di Indonesia

Arvi Erawan Palindria [a,1], Muhammad Sulthan Thufail [b,2], Muhammad Rieval Febrian[c,3]
[a]Universitas Padjadjaran, Indonesia
[b]Universitas Padjadjaran, Indonesia
[c]Universitas Padjadjaran, Indonesia
[1] arvi21001@mail.unpad.ac.id; [2] muhammad23103@mail.unpad.ac.id;
[3]muhammad23306@mail.unpad.ac.id
**email korespodensi:* arvi21001@mail.unpad.ac.id

INFORMASI ARTIKEL

Sejarah Artikel
Diserahkan
2024-08-24
Diterima
2024-10-09
Dipublikasikan
2024-10-30

Kata Kunci
Deepfake;
Data Biometrik;
Keamanan;
Peraturan;
Pelindungan

ABSTRAK

Throughout its evolution, artificial intelligence not only has positive impacts on mankind. One of which is Deepfake, an AI model that poses a serious threat to the security of biometric data, which is a type of specific personal data. Regulations regarding biometric data can be found in Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *However, these regulations do not specifically address biometric data. The existence of deepfake, which could manipulate videos and/or photos, becomes a serious threat that needs attention. Therefore, the objective of this research is to identify the threats posed by deepfake technology to biometric data security and the roles of the government and industry in anticipating these threats. This research was conducted using a normative juridical legal research method with a statute approach and a conceptual approach using futuristic interpretation. The findings from this research journal indicate that the absence of specific protection for biometric data security leads to the vulnerability of biometric data to misuse. The government's role is needed to establish* Peraturan Pelaksana Undang-Undang Pelindungan Data Pribadi *and regulation that specifically addresses biometric data.*

1. PENDAHULUAN

Indonesia adalah negara berdaulat yang segala keterkaitannya didasarkan pada hukum *(rechtsstaat)*. Berdasar pada hal tersebut, maka segala sesuatu perbuatan yang dilakukan oleh setiap warga negara harus tunduk dan taat pada hukum yang berlaku. Hukum merupakan suatu instrumen yang sangat penting bagi kehidupan manusia, karena norma hukum berguna untuk mengatur tata perilaku manusia guna mencapai kesejahteraan. Gustav Radbruch menyatakan bahwa hukum ada untuk mencapai tiga (3) tujuan, yaitu: kepastian, keadilan dan kemanfaatan[1]. Berdasarkan hal itu norma hukum perlu dibentuk untuk menciptakan keteraturan dalam masyarakat.

[1] Sudikno Mertokusumo, *Mengenal Hukum* (Yogyakarta: Penerbit Atmajaya, 1999), p.65.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

Perubahan global yang terjadi saat ini membawa dampak yang cukup signifikan dalam kehidupan pada suatu negara. Hal ini tidak terlepas pula dengan yang terjadi di Indonesia. Maraknya penggunaan teknologi dalam kehidupan masyarakat global dan terkhusus masyarakat Indonesia membawa dampak tersendiri. Pada saat ini juga hampir seluruh perilaku manusia di dalam kehidupan bermasyarakat diatur oleh hukum. Pada sisi lain kemampuan hukum dalam mengupayakan menuju negara yang berprinsip pada *welfare state* masih jauh dirasa.

Pada dasarnya, hukum diharapkan mampu untuk dapat selalu memberikan kepastian serta menjadi tempat menemukan jawaban atas segala permasalahan yang dihadapi atau dialami oleh manusia yang merupakan subjek daripada hukum itu sendiri. Dalam perkembangannya saat ini, teknologi telah memegang peranan yang sangat penting dalam perkembangan kehidupan manusia. Pada akhirnya, teknologi pun harus mulai diperhitungkan sebagai variabel yang dapat menentukan keberlanjutan kehidupan manusia. Khususnya dalam negara Indonesia yang sedang menghadapi apa yang disebut "Industrial Revolution 4.0".

Pada perkembangan era teknologi masa kini, banyak ditemukan teknologi yang dibentuk untuk membuat segala aktivitas manusia menjadi praktis dan mudah, contohnya seperti Artificial Intelligence (selanjutnya disebut "AI"). AI merupakan teknologi yang tersusun dalam sistem komputer untuk menyelesaikan masalah dengan mengimitasi tindakan manusia. Tindakan imitasi yang dilakukan AI dapat berbentuk pembelajaran terhadap data-informasi, membentuk kesimpulan, dan pembenahan diri secara mandiri tanpa memerlukan bantuan dari pihak lain[2]. AI memiliki 3 (tiga) tingkat perubahan atau evolusi, yaitu *Artificial Narrow Intelligence* (ANI) yang merupakan bentuk dari AI Lemah, *Artificial General Intelligence* (AGI) atau yang lebih dikenal sebagai AI Kuat yang memiliki kemampuan sebanding dengan manusia, *Artificial Superintelligence* (ASI) merupakan bentuk AI yang secara sengaja diciptakan untuk melampaui kemampuan manusia[3].

Kecerdasan Buatan *(artificial intelligence)* merupakan inovasi baru di bidang ilmu pengetahuan. Mulai ada sejak muncul komputer modern, yakni pada 1940 dan 1950. Kemampuan mesin elektronika baru menyimpan sejumlah besar info, memproses dengan kecepatan sangat tinggi menandingi kemampuan manusia. Ilmu pengetahuan komputer ini khusus ditujukan dalam perancangan otomatisasi tingkah laku cerdas dalam sistem kecerdasan komputer. Pada sistem ini memperlihatkan sifat-sifat khas yang dihubungkan dengan kecerdasan dalam kelakuan yang sepenuhnya dapat menirukan beberapa fungsi otak manusia, seperti pengertian bahasa, pengetahuan, pemikiran, pemecahan, dan masalah.

Menurut H.A. Simon (1987) dalam jurnal Harihayati & Kurnia (2012), kecerdasan buatan *(artificial intelligence)* merupakan kawasan penelitian, aplikasi, dan instruksi yang terkait dengan pemrograman komputer untuk melakukan hal yang dalam pandangan manusia adalah cerdas. Bidang-bidang yang termasuk dalam kecerdasan buatan antara lain adalah sistem pakar *(expert system)*, robotika *(robotics)*, pengolahan bahasa alami *(language processing)*, pengenalan ucapan *(speech Recognition)*, dan jaringan saraf tiruan *(neural network)*[4].

---

[2] Rafki Fachrizal, 'Apa Itu Teknologi Artificial Intelligence?' *infokomputer.grid.id* <https://infokomputer.grid.id/read/12878703/apaitu-teknologi-artificial-intelligence?page=all> [accessed 26 Juli 2024)

[3] Ashshidqi, M. D., *Proyeksi Dampak Teknologi Artificial General Intelligence dan Tanggung Jawab Ilmuwan* (Yogyakarta: Universitas Gadjah Mada, 2019), p. 36.

[4] T Harihayati, L Kurnia, 'SISTEM PAKAR MENDIAGNOSA PENYAKIT UMUM YANG SERING DIDERITA BALITA BERBASIS WEB DI DINAS KESEHATAN KOTA BANDUNG', *KOMPUTA: Jurnal Ilmiah Komputer dan Informatika*, 1.1 (2012), p. 66, <http://repository.unikom.ac.id/id/eprint/30231>.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

Hingga saat ini, AI sudah digunakan pada berbagai sektor seperti perdagangan, kesehatan, hukum, dan politik. Hal ini membuktikan bahwa AI sudah digunakan dalam berbagai bidang kehidupan masyarakat. Akan tetapi, Pasal 1 angka 8 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatakan bahwa Agen Elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang[5]. Berdasarkan definisi tersebut, dapat dikatakan bahwa posisi AI saat ini merupakan agen elektronik, karena AI yang masih dioperasikan oleh seseorang yang menghendaki sebuah tindakan tertentu dengan menggunakan AI. Jika terdapat perkembangan AI yang melampau tindakan manusia, maka definisi Pasal 1 angka 8 UU ITE tidak lagi bisa digunakan sebagai landasan pengaturan AI di Indonesia.

Kecerdasan Buatan (AI) dan data pribadi memiliki hubungan yang erat dan kompleks. Di satu sisi, AI membutuhkan data pribadi dalam jumlah besar untuk dilatih dan dioptimalkan. Di sisi lain, penggunaan AI untuk memproses dan menganalisis data pribadi menimbulkan kekhawatiran tentang privasi dan keamanan data. Termasuk dalam salah satu jenis data pribadi, yaitu data biometrik. Data Biometrik adalah data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA[6].

Data biometrik merupakan data yang di dalamnya terdapat keterangan dari karakteristik dari pemilik data tersebut yang bersifat benar dan nyata, yaitu suatu data yang didalamnya terdapat karakteristik fisiologi dari suatu individu[7]. Karakteristik data biometrik yang hanya melekat pada pemilik data merupakan karakteristik yang menjadi pembeda data biometrik dari jenis data lainnya. Karakteristik tersebut menimbulkan sifat data biometrik yang unik, sulit dipalsukan, cenderung permanen, dan lain sebagainya[8]. Data biometrik merupakan data yang di dalamnya terdapat karakteristik dari pemilik data, baik karakteristik sifat maupun fisik[9]. Adanya karakteristik pemilik data, data biometrik menjadi data yang hanya melekat pada pemilik data yang menjadikan alasan penggunaan data biometrik di bidang keamanan dan otentitas.

Penggunaan AI dan data biometrik memang sering ditemukan pada sistem keamanan dan otentitas. Dengan karakteristik data biometrik yang hanya melekat pada pemilik data, AI dapat memaksimalkan kinerja data biometrik untuk meningkatkan efektivitas dan ketepatan data, yang mana akan meningkatkan keamanan serta otentitas[10]. Terlepas dari keamanan dan otentitas yang diberikan dari penggunaan kedua teknologi tersebut, penggunaan AI dan data biometrik secara bersamaan menimbulkan permasalahan tersendiri. Salah satunya timbul dari kemampuan AI

[5] Pasal 1 angka 8 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[6] Penjelasan Pasal 4 ayat (2) Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi.

[7] Mohammad Thoriq Bahri, 'Immigration Biometric Data Exchange Among Asean Member States: Opportunities And Challenges In Legislations', *Jurnal Ilmiah Kebijakan Hukum,* 15.3 (2022), p. 443, <https://ssrn.com/abstract=4292444>.

[8] Lawrence J. Fennelly, *Effective Physical Security* (Oxford: Elsevier Inc., 2013), p. 255.

[9] Muhammad Adin Palimbani, 'Polemik Keamanan Data Biometrik", <https://gc.ukm.ugm.ac.id/2020/08/polemik-keamanandata-biometrik/> [accessed 27 Juli 2024].

[10] Alex Vasilchenko, 'Biometric Authentication for Enterprise Security', *mobidev.biz* <https://mobidev.biz/blog/ai-biometrics-technologyauthentication-verificationsecurity#:~:text=Physical%20Biometric%20Technology&text=One%20of%20the%20cases%20where,matching%20them%20with%20a%20database> [accessed 27 Juli 2024].

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

untuk bertindak secara mandiri tanpa memerlukan intervensi dari pihak lain. Atas kemampuan tersebut AI dapat mengumpulkan data dari sumber-sumber yang ada secara mandiri tanpa perlu bantuan manusia[11]. AI dapat mengumpulkan data biometrik tanpa persetujuan dari pemilik data biometrik tersebut. Hal tersebut menimbulkan kemungkinan terjadinya penggunaan data di luar tujuan *(data repurposing)* dan pengumpulan data di luar keperluan *(data spillover)* yang menjadi problematika terhadap pelindungan data pribadi[12].

Dengan kemajuan teknologi kecerdasan buatan (AI), muncullah ancaman baru, yaitu *deepfake*. Penggunaan *deepfake* untuk menipu sistem biometrik dapat menimbulkan berbagai konsekuensi serius. Teknologi *deepfake* ini merupakan teknologi AI yang digunakan untuk memanipulasi atau menipu sebuah objek baik berupa gambar atau video[13]. *Deepfake* dianggap sebagai hiburan bagi masyarakat apabila ditinjau dari sisi positifnya. Namun, jika ditinjau dari sisi negatifnya, maka teknologi *deepfake* ini mengakibatkan terjadinya tindakan penyebarluasan asusila yang mengundang SARA, peretasan terhadap data informasi *(hacking)*, dan penyebaran berita bohong atau tidak benar *(hoax)*[14]. Kemunculan teknologi *deepfake* di kalangan masyarakat khususnya di kalangan masyarakat Indonesia memunculkan sebuah permasalahan ujaran kebencian dan berita bohong yang semakin meningkat secara cepat. Berita hoaks secara digital bisa disampaikan dari berbagai lini teknologi, misalnya adalah dengan media sosial. Dengan demikian, teknologi deepfake buatan AI menimbulkan permasalahan hukum karena memberikan ancaman terhadap keamanan data biometrik di Indonesia. Akibatnya, permasalahan tersebut menimbulkan dua pertanyaan dalam artikel ini, yaitu:

1. Bagaimana ancaman yang ditimbulkan oleh adanya teknologi *deepfake* terhadap keamanan data biometrik?
2. Bagaimana peran pemerintah dan industri dalam melindungi data biometrik serta langkah-langkah yang dapat diambil untuk melindungi data biometrik dari ancaman *deepfake*?

2. METODE PENELITIAN

Penelitian dengan judul "Analisis Yuridis Mengenai Potensi *Deepfake* Buatan AI Mengancam Keamanan Data Biometrik di Indonesia" dianalisis dengan metodologi Yuridis Normatif melalui Pendekatan Perundang-Undangan *(Statute Approach)* dan Pendekatan Konseptual *(Conceptual Approach)* dengan menggunakan Interpretasi Futuristis. Sumber data yang digunakan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer meliputi peraturan perundang-undangan yang memiliki keterkaitan dengan semua peraturan perundang-undangan di Indonesia yang relevan dengan teknologi, AI, dan pelindungan data biometrik. Data sekunder mencakup buku-buku, jurnal ilmiah, artikel, laporan penelitian, dan dokumen-dokumen lain yang masih memiliki relevansi dengan topik penelitian.

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi literatur dan analisis

---

[11] Shehmir Javaid, 'Data Collection Automation: Pros, Cons, & 3 Methods in 2023' *aimultiple.com* <https://research.aimultiple.com/data-collection-automation> [accessed 27 Juli 2024].

[12] Guy Pearce, 'Beware the Privacy Violations in Artificial Intelligence Applications', *isaca.org* <https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificialintelligence-applications>.

[13] Rahayu, R. A. S., & Santoso, H, 'ANALISIS GAMBAR WAJAH PALSU: MENDETEKSI KEASLIAN GAMBAR YANG DIMANIPULASI MENGGUNAKAN METODE VARIATIONAL AUTOENCODER DAN FORENSICS DEEP NEURAL NETWORK', *SIBATIK JOURNAL* 2.9 (2023), p. 2703 <https://doi.org/10.54443/sibatik.v2i9.1312>.

[14] Faqih, M., & Soerjati Priowirjanto, E, 'Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia', *Jurnal Indonesia Sosial Teknologi* 3.11 (2022), p. 1159, <https://doi.org/10.59141/jist.v3i11.528> .

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

isi. Studi literatur dilakukan dengan mengumpulkan dan membaca literatur hukum dan non-hukum yang relevan dengan topik penelitian, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan literatur lainnya. Analisis isi dilakukan terhadap peraturan perundang-undangan dan literatur hukum dan non-hukum lain untuk mengidentifikasi norma-norma hukum yang relevan untuk memahami implikasinya terhadap pelindungan data biometrik dalam konteks perkembangan teknologi AI dan *deepfake*. Dengan mengintegrasikan kedua pendekatan tersebut, penelitian ini akan menghasilkan identifikasi potensi ancaman dan langkah pencegahan pelanggaran keamanan data biometrik di Indonesia akibat dari adanya *deepfake*.

3. HASIL DAN PEMBAHASAN

3.1 Penggunaan *Deepfake* Untuk Menipu Data Biometrik

Deepfake adalah video atau gambar yang dimanipulasi menggunakan kecerdasan buatan (AI) untuk menampilkan seseorang seolah-olah mengatakan atau melakukan sesuatu yang tidak pernah mereka lakukan. Teknologi ini dapat digunakan untuk berbagai tujuan, termasuk penipuan, pemerasan, dan penyebaran informasi yang salah. Salah satu potensi bahaya terbesar dari *deepfake* adalah kemampuannya untuk menipu sistem biometrik. Sistem biometrik menggunakan berbagai teknik untuk mengidentifikasi individu berdasarkan karakteristik fisik mereka, seperti sidik jari, wajah, dan iris mata. *deepfake* dapat digunakan untuk membuat replika wajah seseorang yang sangat realistis, sehingga dapat menipu sistem biometrik untuk berpikir bahwa replika tersebut adalah orang yang sebenarnya.

Deepfake sebagai teknik manipulasi media berbasis kecerdasan buatan (AI) telah mengalami evolusi pesat. Tahap awal ditandai dengan munculnya *FakeApp*, yaitu perangkat lunak yang memerlukan dataset besar untuk menghasilkan model wajah target. Proses ini melibatkan ekstraksi gambar dan video untuk menciptakan konten palsu yang meyakinkan. Selanjutnya, teknik *Deepfake Expression Dynamic (DDE)* muncul dengan kemampuan rekonstruksi detail yang lebih tinggi melalui sistem presisi waktu. Teknik ini menghasilkan representasi wajah palsu yang lebih halus dan realistis.

Generasi *deepfake* berikutnya melibatkan pelacakan model wajah parametrik menggunakan input RGB-D, dengan pencahayaan khusus pada area mulut untuk meningkatkan detail ekspresi. Pendekatan ini menghasilkan gambar yang lebih akurat dan mendekati realitas dibandingkan teknik sebelumnya. Perkembangan pesat teknologi informasi dan AI ini menghadirkan tantangan signifikan. Ketergantungan berbagai sektor pada sistem informasi digital meningkatkan kerentanan terhadap ancaman manipulasi media dan disinformasi. Oleh karena itu, pengembangan metode deteksi dan mitigasi *deepfake* menjadi krusial untuk menjaga integritas informasi dan kepercayaan publik. Hal ini dikarenakan hampir semua elemen baik pemerintahan, perusahaan, dan masyarakat menggunakan serta bergantung pada sistem informasi digital sehingga rentan terhadap ancaman.

Masalah penggunaan dari *deepfake* ini semakin bermunculan secara luas dan beragam. Contoh terkenal dari video *deepfake* ini adalah video Barack Obama menyebut Donald Trump sebagai "orang yang *total and complete dip*****" [15]. Video ini memberikan peringatan bahwa penggunaan *deepfake* sangat berisiko tinggi dan berbahaya, pengguna harus lebih hati-hati dan bijak dalam menggunakan media internet dewasa ini. Masalah selanjutnya dari *deepfake*

[15] Barari, S., Lucas, C., & Munger, K, 'Political Deepfakes Are As Credible As Other Fake Media And (Sometimes) Real Media', *OSF Preprints* 13 (2021) <https://doi.org/10.31219/osf.io/cdfh3>.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

ini adalah untuk tujuan pornografi. Dari sebuah penelitian yang dilakukan oleh perusahaan keamanan siber Deeptrace yang diterbitkan pada Oktober 2019, terdapat 95% video palsu yang bersifat pornografi. Mayoritas dalam penggunaanya terdapat menyamarkan wajah korban. Dalam hal ini asalkan tercukupi gambar wajah korban, maka penukaran wajah dapat digunakan untuk membuat *deepfake* siapa saja. Ilustrasi menarik lainnya adalah audio John F. Kennedy saat menyampaikan pidato yang akan disampaikan di Dallas pada tanggal 22 November 1963. Audio tersebut diproduksi oleh sebuah perusahaan sintetis canggih Cereproc dan disajikan pada bulan Maret 2018, pidato yang akan disampaikan Kennedy seandainya dia tidak tertembak[16].

Kekhawatiran selanjutnya muncul di dunia stabilitas pasar keuangan. Westerlund menyoroti bahwa teknologi AI yang canggih telah digunakan untuk membuat audio palsu dari para CEO yang meminta bantuan tunai mendesak. Hal ini dapat terjadi karena perkembangan teknologi pemalsuan identitas secara *real-time* akan segera menjadi mungkin sebuah kriminal. Fenomena *deepfake* yang telah diuraikan di atas, secara umum muncul akibat permasalahan yang komprehensif di lingkungan masyarakat. Permasalahan ini pada dasarnya muncul dari kepentingan-kepentingan, baik dari kepentingan pribadi, golongan, maupun sosial budaya dan didorong dengan munculnya perkembangan teknologi yang tak terbendung. Hal inilah yang memicu fenomena *deepfake* di masyarakat bermunculan.

Meskipun tinjauan ini tidak mencakup semua aspek penggunaan teknologi *deepfake*, tetapi telah mengilustrasikan potensi masalah etika yang signifikan. Dampak negatif *deepfake* dapat meluas, termasuk krisis kepercayaan terhadap institusi demokrasi, peningkatan ketegangan sosial dan politik, kejahatan, gangguan stabilitas pasar keuangan, kerusakan hubungan diplomatik, dan bahkan memicu kekerasan. Meskipun *deepfake* memiliki potensi penggunaan positif, implikasi penelitian mendalam dan perkembangan teknologi ini menekankan pentingnya pemeriksaan etika yang cermat terhadap penggunaan teknologi dan hasilnya. Hal ini bertujuan untuk memastikan validitas dan kebenaran informasi yang dihasilkan, serta mencegah penyalahgunaan yang dapat merugikan individu, masyarakat, dan institusi. Oleh karena itu, diperlukan pendekatan holistik yang melibatkan regulasi, pengembangan teknologi deteksi, serta edukasi publik untuk memaksimalkan manfaat *deepfake* sambil memitigasi risiko dan dampak negatifnya.

Pentingnya literasi digital yang komprehensif untuk menyaring informasi secara efektif dan menghindari hoaks, terutama dengan maraknya teknologi *deepfake* berbasis AI. Sejalan dengan penelitian Gandrova & Banke (2023) dan Hailtik & Afifah (2024) yang menyampaikan bahwa guna menghentikan penyebaran disinformasi dari hasil olahan *deepfake* diperlukan peran tanggap dari petugas polisi dan pemerintah diikuti dengan perlindungan siber dan payung hukum yang lebih ketat. Akan tetapi, karena AI belum diakui sebagai subjek hukum sehingga apabila melakukan tindak pidana, maka yang harus bertanggung jawab adalah pencipta AI atau pengguna AI.

Oleh karena itu, solusi yang diusulkan adalah meningkatkan keterampilan fungsional dalam penggunaan alat digital secara efektif dan bijaksana, termasuk kemampuan adaptasi terhadap teknologi baru. Selain itu, penting untuk mengembangkan kemampuan berpikir kritis dalam mengevaluasi kebenaran informasi, dengan memahami asumsi dasar yang mendasari proses pembuatan informasi tersebut. Penguasaan literasi digital juga memungkinkan individu untuk mengakses, memahami, menyebarkan, membuat, dan memperbarui konten digital secara

16 Floridi, L., 'Artificial Intelligence, Deepfakes and a Future of Ectypes in: floridi, l. (eds) Ethics, Governance, and Policie in Artificial Intelligence', *Philosophical Studies Series*, 144 (2022), <https://doi.org/10.1007/978-3-030-81907-1_17>.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

efektif, sehingga dapat mengambil keputusan yang tepat dalam kehidupan mereka. Dengan keterampilan ini, individu dapat memanfaatkan media digital untuk tujuan produktif dan pengembangan diri, bukan untuk kegiatan konsumtif atau destruktif.

3.2 Kurangnya Pelindungan Hukum Terhadap Data Biometrik di Indonesia

Undang-Undang Pelindungan Data Pribadi mencakup data biometrik sebagai bagian dari data pribadi yang bersifat spesifik bersamaan dengan data lainnya seperti data informasi Kesehatan, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan data lainnya. Definisi mengenai data biometrik terdapat di Penjelasan atas Pasal 4 ayat (2) huruf b UU PDP. Akan tetapi, UU PDP belum mengatur lebih jelas mengenai data biometrik. UU PDP hanya memberi definisi mengenai data biometrik secara singkat. Tidak ada penjelasan secara spesifik mengenai hal-hal yang termasuk ke dalam data biometrik, juga tidak ada penjelasan mengenai bagaimana cara memperoleh, mengolah, menyimpan, memperbaiki, maupun menghapus/memusnahkan data biometrik. Ruang lingkup mengenai data biometrik yang terdapat di UU PDP terhitung masih terlalu sedikit. Dengan terbatasnya penjelasan mengenai data biometrik di UU PDP, maka hal ini menimbulkan ketidakpastian hukum mengenai Pelindungan data biometrik di Indonesia.

UU PDP tidak dapat memberikan pelindungan hukum yang jelas dan spesifik terhadap keamanan data biometrik. Walaupun data biometrik merupakan data pribadi yang termasuk ke dalam ruang lingkup pengaturan data pribadi. Akan tetapi, pelindungan secara umum yang dilakukan terhadap data pribadi yang spesifik membuat keamanan data biometrik di Indonesia menjadi rentan akan penyalahgunaan. Tidak ada penjelasan secara spesifik mengenai hal-hal yang termasuk ke dalam data biometrik, seperti mengenai cara memperoleh, mengolah, menyimpan, memperbaiki, maupun menghapus atau memusnahkan data biometrik. Peraturan yang mengenai data biometrik di Indonesia belum diatur secara khusus. Dengan tidak adanya regulasi yang secara khusus mengatur mengenai data biometrik akan membuat masyarakat lebih rentan terhadap ancaman-ancaman yang ada. Pengaturan tersebut ditujukan guna melindungi data pribadi yang bersifat spesifik. Karena data pribadi yang bersifat spesifik dalam pemrosesannya dapat mengakibatkan dampak dan kerugian yang lebih besar kepada subjek data pribadi.[17]

Kerugian yang ditimbulkan dari adanya penyalahgunaan data pribadi yang bersifat spesifik dapat berasal dari adanya ancaman-ancaman terhadap penyalahgunaannya. Ancaman tersebut salah satunya adalah *deepfake.* Ancaman yang ditimbulkan dengan adanya *deepfake* terhadap keamanan data biometrik merupakan masalah yang serius. Sehingga diperlukan aturan yang dapat melindungi keamanan data biometrik secara khusus. Dengan demikian, dasar hukum dari pelindungan data biometrik di Indonesia menimbulkan kepastian hukum akan pelaksanaannya. Dengan adanya kepastian hukum tersebut akan menimbulkan konsekuensi yang jelas bilamana terjadi suatu pelanggaran atau kejahatan di kemudian hari.

3.3 Peran Pemerintah dalam Melindungi Data Biometrik dari Ancaman *Deepfake*

Deepfake mengacu pada video yang direkayasa oleh AI dengan begitu meyakinkan sehingga berpotensi menyesatkan penonton, menciptakan hoaks, dan melakukan penipuan. *Deepfake* yang ditemukan kebanyakan menggunakan wajah orang yang sesungguhnya. Suaranya mirip, tetapi yang dibicarakan tidak sesuai dengan karakter orang tersebut. Untuk mengatasi hal ini, tentunya pemerintah perlu membuat peraturan pelaksana dari UU PDP yang jelas tentang pengumpulan, penyimpanan, dan penggunaan data biometrik. Regulasi ini harus memastikan bahwa data biometrik hanya dikumpulkan dan digunakan untuk tujuan yang sah dan dengan

[17] Penjelasan Pasal 4 Ayat (1) huruf a Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

persetujuan individu. Regulasi juga harus mengatur tentang penggunaan teknologi biometrik untuk mencegah penipuan dan penyalahgunaan data.

Tidak hanya mengenai regulasinya saja, melainkan Pemerintah perlu memperkuat penegakan hukum terhadap penyalahgunaan data biometrik. Hal ini dapat dilakukan dengan meningkatkan kapasitas aparat penegak hukum dan memberikan sanksi yang tegas bagi para pelaku penyalahgunaan data. Karena hukum yang kuat akan menjadi lebih optimal bilamana didukung oleh proses penegakan hukum yang dilakukan oleh sumber daya manusia yang terakreditasi dengan baik. Pemerintah juga perlu meningkatkan kesadaran masyarakat tentang potensi risiko penyalahgunaan data biometrik dan bagaimana cara melindungi diri mereka. Hal ini dapat dilakukan melalui kampanye edukasi dan sosialisasi kepada masyarakat.

Tindakan nyata telah dilakukan oleh Menteri Komunikasi dan Informatika Budi Arie Setiadi telah mengeluarkan surat edaran tentang etika penggunaan AI yang ditujukan kepada para pelaku usaha di ranah publik dan swasta. Edaran tersebut berisikan:[18]

a. Penyelenggaraan kemampuan Kecerdasan Artifisial mencakup kegiatan konsultasi, analisis, dan pemrograman. Penggunaan teknologi Kecerdasan Artifisial termasuk ke dalam subset dari *machine learning, natural language processing, expert system, deep learning, robotics, neural networks*, dan subset lainnya.
b. Penyelenggaraan teknologi Kecerdasan Artifisial memperhatikan nilai Etika Kecerdasan Artifisial meliputi:
    1) Inklusivitas
    Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan nilai kesetaraan, keadilan, dan perdamaian dalam menghasilkan informasi maupun inovasi untuk kepentingan bersama.
    2) Kemanusiaan
    Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan nilai kemanusiaan dengan tetap saling menjaga hak asasi manusia, hubungan sosial, kepercayaan yang dianut, serta pendapat atau pemikiran setiap orang.
    3) Keamanan
    Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan aspek keamanan pengguna dan data yang digunakan agar dapat menjaga privasi, data pribadi, dan mengutamakan hak pengguna Sistem Elektronik sehingga tidak ada pihak yang dirugikan.
    4) Aksesibilitas
    Penyelenggaraan Kecerdasan Artifisial bersifat inklusif dan tidak diskriminatif. Setiap pengguna memiliki hak yang sama dalam mengakses penyelenggaraan teknologi berbasis Kecerdasan Artifisial untuk kepentingannya dengan tetap menjaga prinsip etika Kecerdasan Artifisial yang berlaku.
    5) Transparansi
    Penyelenggaraan Kecerdasan Artifisial perlu dilandasi dengan transparansi data yang digunakan untuk menghindari penyalahgunaan data dalam mengembangkan inovasi teknologi. Pelaku Usaha dan PSE dapat memberikan akses kepada pengguna yang berhak untuk mengetahui penyelenggaraan data dalam pengembangan teknologi berbasis Kecerdasan Artifisial.
    6) Kredibilitas dan Akuntabilitas
    Penyelenggaraan Kecerdasan Artifisial perlu mengutamakan kemampuan dalam pengambilan Keputusan dari informasi atau inovasi yang dihasilkan. Informasi yang

[18] Lihat bagian isi edaran, Surat Edaran Kementerian Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

dihasilkan melalui Kecerdasan Artifisial harus dapat dipercaya dan dipertanggungjawabkan ketika disebarkan kepada publik.

7) Pelindungan Data Pribadi
   Penyelenggaraan Kecerdasan Artifisial harus memastikan pelindungan data pribadi sesuai ketentuan peraturan perundang-undangan.
8) Pembangunan dan Lingkungan Berkelanjutan
   Penyelenggaraan Kecerdasan Artifisial mempertimbangkan dengan cermat dampak yang ditimbulkan terhadap manusia, lingkungan, dan makhluk hidup lainnya, untuk mencapai keberlanjutan dan kesejahteraan sosial.
9) Kekayaan Intelektual
   Penyelenggaraan Kecerdasan Artifisial tunduk pada prinsip pelindungan Hak Kekayaan Intelektual sesuai ketentuan peraturan perundang-undangan.

c. Pelaksanaan dan Tanggung Jawab
   1) Pelaksanaan
      a) Penyelenggaraan Kecerdasan Artifisial dilandasi dengan etika dan kode etik yang berlaku bagi Pelaku Usaha dan PSE.
      b) Pelaksanaan program edukasi terkait Penyelenggaraan Kecerdasan Artifisial meliputi namun tidak terbatas pada pengembangan kompetensi teknis, studi aspek etika, humaniora dan sosial yang dilakukan untuk masyarakat, sebagai tanggung jawab pengembang untuk turut mengembangkan sumber daya manusia di Indonesia.
      c) Penyelenggaraan kemampuan pemrograman berbasis Kecerdasan Artifisial sebagai pendukung aktivitas manusia.
      d) Pengawasan dilakukan oleh pemerintah, penyelenggara, dan pengguna untuk mencegah adanya penyalahgunaan dan/atau pemanfaatan teknologi berbasis Kecerdasan Artifisial yang melanggar ketentuan peraturan perundang-undangan.
      e) Pemanfaatan fasilitas Kecerdasan Artifisial untuk meningkatkan kreativitas pengguna dalam menyelesaikan permasalahan dan pekerjaan.
      f) Penyelenggaraan Kecerdasan Artifisial yang saling menjaga privasi data sehingga tidak ada individu yang dirugikan.
   2) Tanggung Jawab
      a) Memberikan pelindungan kepada masyarakat dalam penyelenggaraan Kecerdasan Artifisial, khususnya terkait dengan penggunaan data.
      b) Memastikan Kecerdasan Artifisial tidak diselenggarakan sebagai penentu kebijakan dan/atau pengambil keputusan yang menyangkut kemanusiaan.
      c) Mencegah adanya rasisme dan segala bentuk tindakan yang merugikan manusia.
      d) Menyelenggarakan Kecerdasan Artifisial untuk peningkatan kemampuan berinovasi dan pemecahan masalah.
      e) Melaksanakan kewajiban regulasi Penyelenggaraan Kecerdasan Artifisial dengan tujuan menjaga keamanan dan hak pengguna di media digital.
      f) Memberikan informasi yang berkaitan dengan pengembangan teknologi berbasis Kecerdasan Artifisial oleh pengembang untuk mencegah dampak negatif dan kerugian dari teknologi yang dihasilkan terhadap pengguna, Kementerian Komunikasi dan Informatika, dan/atau publik.
      g) Memperhatikan manajemen risiko dan manajemen krisis dalam pengembangan Kecerdasan Artifisial.

Dengan adanya surat edaran ini, perusahaan pengelola AI dapat dibatasi oleh pemerintah. Pengguna juga tidak bisa sembarangan menggunakan AI untuk hal-hal yang tidak jelas. Apalagi jika menggunakannya untuk melakukan pelanggaran, seperti pelanggaran data pribadi dengan menggunakan teknologi *deepfake*.

3.4 Peran Industri dalam Melindungi Data Biometrik dari Ancaman *Deepfake*

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

Dalam peranannya, perusahaan pengelola atau penyedia layanan digital harus menggunakan teknologi biometrik yang aman dan tahan terhadap manipulasi. Hal ini dapat dilakukan dengan menggunakan teknologi biometrik multi-faktor yang menggabungkan beberapa jenis data biometrik, seperti sidik jari dan wajah. Perusahaan harus memperkuat keamanan siber mereka untuk melindungi data biometrik dari akses yang tidak sah dan kebocoran data. Hal ini dapat dilakukan dengan menerapkan berbagai langkah keamanan seperti enkripsi data, kontrol akses yang ketat, dan audit keamanan secara berkala.

Harus adanya penerapan kebijakan privasi yang ketat dan transparan dari perusahaan tentang bagaimana mereka mengumpulkan, menyimpan, dan menggunakan data biometrik sesuai dengan yang diatur dalam UU PDP. Kebijakan ini harus menjelaskan kepada pelanggan bagaimana data mereka digunakan dan bagaimana mereka dapat mengontrolnya. Serta berkolaborasi dengan pemerintah untuk mengembangkan standar dan praktik terbaik untuk melindungi data biometrik. Hal ini dapat dilakukan dengan berpartisipasi dalam forum diskusi dan penelitian tentang keamanan biometrik.

3.5 Langkah-langkah Pelindungan Data Biometrik dari Ancaman *Deepfake*

a. Menghindari membagikan informasi biometrik, seperti foto dan video, secara online.
b. Gunakan kata sandi yang kuat dan unik untuk akun yang menggunakan data biometrik.
c. Aktifkan autentikasi dua faktor untuk menambahkan lapisan keamanan ekstra.
d. Gunakan perangkat lunak antivirus untuk melindungi perangkat Anda dari malware yang dapat mencuri data biometrik.
e. Tetap *up-to-date* dengan berita dan perkembangan terbaru tentang penipuan biometrik dan bagaimana cara melindungi diri dari ancaman deepfake.
f. Pilihlah perangkat lunak pengenalan wajah yang andal dan memiliki reputasi baik.
g. Laporkan aktivitas mencurigakan kepada pihak berwenang jika terdapat hal-hal mencurigakan terkait data biometrik dengan dugaan terdapat sesuatu pihak yang menyalahgunakannya.

4. KESIMPULAN

Deepfake mengacu pada teknologi AI yang mampu merekayasa video dan/atau foto menggunakan data biometrik dengan sangat meyakinkan. Dengan kemampuan replika wajah dan pemalsuan identitas yang canggih menimbulkan ancaman yang nyata. Konsekuensi yang berpotensi muncul diantaranya penipuan identitas, pelanggaran privasi, dan akses ilegal terhadap informasi sensitif. Selain itu, ditemukan kasus manipulasi audio palsu yang memungkinkan terjadi pencemaran nama baik seseorang. *Deepfake* juga paling banyak digunakan dalam pembuatan video pornografi palsu dengan mengganti wajah seseorang tanpa adanya persetujuan.

Data biometrik yang termasuk dalam data spesifik tidak memiliki regulasi spesifik yang mengaturnya. Tidak adanya pelindungan secara khusus membuat data biometrik rentan akan penyalahgunaan. Proses terkait data spesifik itu sendiri berpotensi mengakibatkan kerugian yang signifikan bagi subjek data pribadi. Di samping itu, pemerintah telah mengeluarkan surat edaran mengenai etika penggunaan AI bagi para pengusaha di ranah publik dan swasta. Surat edaran tersebut menyatakan kegiatan konsultasi, analisis, dan pemrograman sebagai bagian dari penyelenggaraan AI. Termasuk juga di dalamnya ialah nilai etika kecerdasan artifisial yang mencakup inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, pelindungan data pribadi, pembangunan dan lingkungan berkelanjutan, serta kekayaan intelektual. Tercantum pula langkah pelaksanaan dan pertanggungjawaban para pelaku usaha terkait pemanfaatan AI. Meskipun demikian, adanya surat edaran hanya mengikat secara umum dan bukan sebagai dasar hukum yang mengikat dengan suatu peraturan

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

perundang-undangan. Pelindungan data biometrik tetap memerlukan regulasi khusus yang mengatur segala hal dan proses di dalamnya. Dengan demikian, pelindungan data biometrik dapat dilakukan secara komprehensif dan optimal.

Oleh karena itu, peran pemerintah sangat dibutuhkan untuk membuat peraturan pelaksana UU PDP dan peraturan perundang-undangan yang secara khusus mengatur data biometrik. Penegakkan hukum yang tegas terhadap penyalahgunaan data biometrik juga perlu dioptimalkan guna mencegah kerugian yang ditimbulkan. Industri sebagai pihak penyedia layanan juga perlu untuk menerapkan sistem biometrik yang aman dari ancaman manipulasi data. Dengan menerapkan kebijakan privasi yang ketat dan transparan serta memperkuat keamanan siber diharapkan bisa meminimalisasi adanya kebocoran data dan akses ilegal. Hal ini dapat tercapai apabila pihak industri menerapkan enkripsi data, kontrol akses yang ketat, serta audit keamanan secara berkala. Kesadaran masyarakat sebagai pengguna turut diharapkan sebagai upaya menjaga keamanan data biometrik dalam kaitannya dengan penggunaan teknologi *deepfake*. Berhati-hati dalam membagikan informasi biometrik, memantau perkembangan terbaru mengenai isu *deepfake,* serta melaporkan aktivitas mencurigakan adalah beberapa langkah yang perlu dilakukan.

DAFTAR PUSTAKA

Ashshidqi, M. D., *Proyeksi Dampak Teknologi Artificial General Intelligence dan Tanggung Jawab Ilmuwan* (Yogyakarta: Universitas Gadjah Mada, 2019)

Bahri, Mohammad Thoriq, 'Immigration Biometric Data Exchange Among Asean Member States: Opportunities And Challenges In Legislations', *Jurnal Ilmiah Kebijakan Hukum,* 15.3 (2022) <https://ssrn.com/abstract=4292444>

Barari, S., Lucas, C., & Munger, K, 'Political Deepfakes Are As Credible As Other Fake Media And (Sometimes) Real Media', OSF Preprints 13 (2021) <https://doi.org/10.31219/osf.io/cdfh3>

Fachrizal, Rafki 'Apa Itu Teknologi Artificial Intelligence?' *infokomputer.grid.id* <https://infokomputer.grid.id/read/12878703/apaitu-teknologi-artificial-intelligence?page=all> [accessed 26 Juli 2024]

Faqih, M., & Soerjati Priowirjanto, E, 'Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia', Jurnal Indonesia Sosial Teknologi 3.11 (2022), p. 1159, <https://doi.org/10.59141/jist.v3i11.528>

Fennelly, Lawrence J., *Effective Physical Security* (Oxford: Elsevier Inc., 2013)

Floridi, L., 'Artificial Intelligence, Deepfakes and a Future of Ectypes in: floridi, l. (eds) Ethics, Governance, and Policie in Artificial Intelligence', Philosophical Studies Series, 144 (2022), <https://doi.org/10.1007/978-3-030-81907-1_17>

Harihayati, T., Kurnia L., 'SISTEM PAKAR MENDIAGNOSA PENYAKIT UMUM YANG SERING DIDERITA BALITA BERBASIS WEB DI DINAS KESEHATAN KOTA BANDUNG', *KOMPUTA: Jurnal Ilmiah Komputer dan Informatika*, 1.1 (2012) <http://repository.unikom.ac.id/id/eprint/30231>

Javaid, Shehmir, 'Data Collection Automation: Pros, Cons, & 3 Methods in 2023' *aimultiple.com* <https://research.aimultiple.com/data-collection-automation> [accessed 27 Juli 2024]

ISSN Print: 1858-0246 | ISSN Online: 2355-1550
Doi : 10.56444/sh.v21i2.5319

Mertokusumo, Sudikno, *Mengenal Hukum* (Yogyakarta: Penerbit Atmajaya, 1999)

Palimbani, Muhammad Adin, 'Polemik Keamanan Data Biometrik", *gc.ukm.ugm.ac.id* <https://gc.ukm.ugm.ac.id/2020/08/polemik-keamanandata-biometrik/> [accessed 27 Juli 2024]

Pearce, Guy, 'Beware the Privacy Violations in Artificial Intelligence Applications', isaca.org <https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificialintelligence-applications> [accessed 27 Juli 2024]

Rahayu, R. A. S., & Santoso, H, 'ANALISIS GAMBAR WAJAH PALSU: MENDETEKSI KEASLIAN GAMBAR YANG DIMANIPULASI MENGGUNAKAN METODE VARIATIONAL AUTOENCODER DAN FORENSICS DEEP NEURAL NETWORK', SIBATIK JOURNAL 2.9 (2023) <https://doi.org/10.54443/sibatik.v2i9.1312>

Surat Edaran Kementerian Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi

Vasilchenko, Alex, 'Biometric Authentication for Enterprise Security', mobidev.biz <https://mobidev.biz/blog/ai-biometrics-technologyauthentication-verificationsecurity#:~:text=Physical%20Biometric%20Technology&text=One%20of%20the%20cases%20where,matching%20them%20with%20a%20database> [accessed 27 Juli 2024]