

PERLINDUNGAN TERHADAP KORBAN PENYALAHGUNAAN TEKNIK *DEEPPAKE* TERHADAP DATA PRIBADI

Vika Oktallia, Fakultas Hukum Universitas Udayana,
e-mail: vikaoktallia@gmail.com

I Gede Putra Ariana, Fakultas Hukum Universitas Udayana,
e-mail: putra_ariana@unud.ac.id

ABSTRAK

Penulisan ini bertujuan untuk mengetahui perlindungan hukum terhadap korban penyalahgunaan data pribadi dengan teknik Deepfake ditinjau dari perspektif pembaharuan hukum pidana melalui metode penelitian yuridis normatif. Teknik deepfake merupakan salah satu contoh nyata kemampuan Artificial Intelligence (AI). Deepfake merupakan suatu teknik untuk menempatkan gambar wajah orang "sebenarnya" dalam suatu video menjadi wajah target sehingga seolah – olah target tersebut melakukan atau mengatakan hal-hal yang dilakukan orang "sebenarnya". Namun sejalan dengan meningkatnya perkembangan teknologi dan informasi tentu memiliki sisi positif dan negatif didalamnya. Dalam sisi negatif Deepfake dapat dipergunakan untuk tujuan seperti propaganda, pornografi atau terkait isu data privasi. Sistem Hukum Indonesia telah mengadopsi instrumen hukum Eropa berupa Right to Be Forgotten (RTBF) yang memiliki arti Hak untuk dilupakan yang diatur di dalam Pasal 26 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai bentuk perlindungan hukum terhadap korban penyalahgunaan data pribadi dengan teknik deepfake.

Kata Kunci: Perlindungan Hukum, Data Pribadi, Teknik Deepfake

ABSTRACT

This study aims to determine the legal protection for the victims of personal data misuse with deepfake technique in terms of the perspectives of criminal law reform through normative judicial research methods. The deepfake technique is one concrete example of the ability of Artificial Intelligence (AI). Deepfake is a technique to place an image of a "real" person's face in a video into a target's face so that it is as if the target is doing or saying things that "real" people do. However, in line with the increasing development of technology and information certainly has positive and negative sides. in negative sides Deepfake can be used for for instance, propaganda, pornography, or any related to data privacy violation. The Indonesian Legal System has adopted a European Legal Instrument in the form of the Right to Be Forgotten (RTBF) which is regulated in Article 26 Paragraph (3) of Law No. 19 of 2016 concerning the Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as a form of legal protection for the victims of personal data misuse with deepfake technique.

Keywords: Legal Protection, Data Privacy, Deepfake Technique

1. Pendahuluan

1.1. Latar Belakang Masalah

Manusia selalu meneliti dan selalu mencari serta menciptakan sistem dan alat yang terhubung untuk saling berhubungan yang dapat mendorong aktivitas mereka.¹ Karena kemajuan teknologi yang pesat, hampir semua fasilitas membutuhkan kecerdasan buatan untuk membuat sesuatu yang efisien dan efektif. Dengan bantuan *Artificial Intelligence* yang selanjutnya akan disebut AI semua perangkat komputer menjadi lebih cerdas dan mempermudah kehidupan sehari-hari manusia. Memang benar jika dikatakan bahwa penggunaan produksi berbasis AI di seluruh dunia sedang meningkat. Bahkan di beberapa negara telah mengimplementasikan AI hingga 56 persen di sektor industrinya. Diperkirakan perusahaan yang mengadopsi AI akan mengalami peningkatan produksi setidaknya 40 persen pada tahun 2023. Strategi Kecerdasan Buatan Nasional Indonesia 2020-2045 telah diterbitkan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) agar AI dapat digunakan secara efektif di Indonesia. Namun, urutannya tidak mengatur secara detail dan masih dalam pedoman kebijakan. Banyak pelaku bisnis di Indonesia yang mengembangkan dan memasukan teknologi AI ke dalam proses produksinya. Hal demikian tidak tanggung-tanggung dimana mayoritas sektor bisnis strategis yang menggunakan AI termasuk layanan kesehatan dan perbankan dan e-commerce. Kenyamanan seperti mengakses dan mempercepat arus informasi, dapat mempercepat kinerja manusia, serta berperan sebagai sarana bisnis dan pendidikan yang juga dapat mendorong masyarakat untuk lebih mengembangkan ide-idenya dalam perkembangan teknologi AI ini.

Namun disamping itu semua, factor yang paling penting yaitu keamanan data dari segi keamanan data pemilik bisnis maupun keamanan data konsumen sama pentingnya. Dalam pengaturan pribadi atau bisnis, kerahasiaan dan keamanan data merupakan masalah penting. Secara alami, ini akan menjadi resiko jika informasi yang berharga dan sensitif dibagikan secara terbuka dengan individu yang tidak berwenang. Informasi keamanan data sistem memainkan peran penting dalam memastikan bahwa keaslian data tidak dapat dengan mudah diubah oleh individu yang tidak bertanggung jawab. Meskipun langkah-langkah keamanan data seperti kata sandi telah di terapkan, peretas masih mungkin mendapatkan akses ke data asli, yang merupakan penyebab umum permasalahan.

Di penghujung Agustus 2019, masyarakat dihebohkan dengan munculnya aplikasi pertukaran wajah bernama Zao. Pengguna mendaftarkan nomor telepon mereka dengan Zao dan mengunggah foto. Pengguna kemudian dapat memilih selebriti yang cocok dengan wajah mereka. Dengan adanya terdapat fenomena yang dapat menciptakan model baru berita palsu, yang bila digunakan untuk tujuan negatif dapat mengancam dan merugikan informasi data pribadi. Fenomena ini dapat menciptakan model baru berita palsu dan, jika digunakan untuk tujuan negatif, dapat mengancam dan membahayakan informasi pribadi seseorang. Di masa lalu, video palsu sering dibuat dengan gambar yang berbeda dari lokasi dan waktu sebenarnya, tetapi kemajuan teknologi telah memungkinkan untuk mengontrol video yang memungkinkan Anda memanipulasi suara dan adegan yang terlihat seperti dibuat oleh seseorang. Menjadi siapa selayaknya Seperti video nyata.² Aplikasi asal China ini menggunakan teknologi *Deepfake*.

¹ Donovan, Typhon Rachmadie. "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016." *Jurnal Recidive Universitas Sebelas Maret* 9 No.2: (2020), 128-129.

² Okezone, 2019, "Viral Aplikasi Tukar wajah ZAO Diduga Curi Data Pengguna", URL: <https://techno.okezone.com/read/2019/09/02/207/2099704/viral-aplikasi-tukar-wajah-zao-diduga-curi-data-pengguna>, dikutip pada 6 Juni 2022.

Deepfake adalah teknik penempatan gambar wajah orang "nyata" dalam video di wajah orang yang dituju, sehingga seolah-olah orang "nyata" sedang melakukan atau mengatakan apa yang dilakukan orang "sebenarnya".³ Jurnalis Josh Brandon dari Fox News menyebut *Deepfake* adalah sebuah istilah yang ramai dibicarakan pada awal tahun 2018 silam, istilah *Deepfake* adalah kependekan dari *deep learning* yaitu suatu pembelajaran mendalam yang merujuk pada kecerdasan buatan dan *fake* atau palsu. *Deepfake* video palsu yang dibuat dengan kajian mendalam. *Deepfake* adalah teknologi berbasis kecerdasan buatan untuk mensintesis gambar manusia yang memungkinkan Anda menggabungkan gambar atau video dengan sumber video menggunakan teknik pembelajaran yang disebut *Generative Adversarial Network* (GAN). Selain itu dampak negatif teknik *Deepfake* antara lain dapat menimbulkan keresahan sosial, menyebarkan kebencian, menjadi alat propaganda, dan dijadikan sebagai alat politik. Dimana sasaran utama atau umum dari penyalahgunaan teknik *Deepfake* adalah tokoh masyarakat dan orang-orang yang menduduki jabatan tinggi. Namun tentunya jika semakin meningkatnya kasus-kasus yang terjadi akibat teknik *deepfake* tersebut maka dapat juga bisa terjadi pada masyarakat umum lainnya.

Hal ini tentu saja akan menimbulkan pertanyaan bagaimana pengaturan penggunaan AI saat ini di Indonesia. Lalu, siapa yang bertanggung jawab atas kerugian yang disebabkan oleh penggunaan AI, serta apa saja perlindungan hukum dan tanggung jawab antara penyedia dan pengguna AI. Berdasarkan uraian diatas, dipandang perlu untuk menyusun penelitian yang diberi judul "**Perlindungan Terhadap Korban Penyalahgunaan Teknik Deepfake Terhadap Data Pribadi**"

1.2. Rumusan Masalah

Setelah memperhatikan pada latar belakang diatas, maka rumusan masalah yang akan dikaji dalam penulisan penelitian ini diantaranya yaitu:

1. Bagaimanakah pengaturan hukum terhadap *Artificial Intelligence* di Indonesia?
2. Apakah terdapat perlindungan terhadap korban penyalahgunaan teknik *deepfake* terhadap data pribadi?

1.3. Tujuan Penelitian

Penulisan Penelitian ini memiliki tujuan yakni sebagai upaya dalam menjawab permasalahan dalam isu yang diangkat oleh penulis pada suatu kajian. Adapun dalam tujuan penulisan ini yaitu untuk menelaah lebih lanjut mengenai pengaturan hukum terhadap *Artificial Intelligence* di Indonesia serta menelaah lebih lanjut mengenai perlindungan Terhadap Korban Penyalahgunaan Tekni *Deepfake* Terhadap Data Pribadi.

2. Metode Penelitian

Metode Penelitian yang digunakan dalam penulisan adalah yuridis normatif dengan menggunakan pendekatan perundang-undangan (*statue approach*) serta pendekatan konseptual (*conceptual approach*). sumber data yang digunakan adalah data sekunder yang terdiri dari bahan hukum primer yaitu bahan-bahan hukum seperti Undang-Undang, bahan hukum sekunder

³ Angelica Roseanne, 2021, "Deepfake Bagaimana Mendeteksinya." URL: <https://informatika.uc.ac.id/id/2021/05/deepfake-bagaimana-mendeteksinya/>, dikutip pada 6 Juni 2022.

yaitu bahan-bahan hukum yang memberikan penjelasan terhadap bahan hukum primer seperti doktrin, karya-karya ilmiah para sarjana, jurnal. Dan bahan hukum tersier yaitu bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder. Analisis data dilakukan secara deskriptif-kualitatif.

3. Hasil dan Pembahasan

3.1. Pengaturan Hukum Terhadap *Artificial Intelligence* di Indonesia

Kemajuan ilmu pengetahuan dan pembangunan di era globalisasi dan modernisasi yang terjadi semakin menuntut. Demikian pula, penyebaran data dan akses ke media komunikasi semakin mudah dan cepat. Internet merupakan konsekuensi dari kemajuan-kemajuan logis dan inovatif buatan manusia, dan keunggulan dari Internet berbeda, salah satunya adalah berkumpulnya jaringan penyelenggara hiburan online.⁴ Perkembangan teknologi informasi yang semakin sederhana akan membawa perubahan sosial. Kelahiran media sosial menjadikan kebiasaan perilaku masyarakat dari budaya ataupun juga etika dan Norma yang berlaku.⁵ Sarana komunikasi seperti media sosial banyak digunakan sebagai alat komunikasi. Sehingga tidak menutup kemungkinan dan juga berpotensi terjadinya pelanggaran data, seperti pencurian informasi pribadi. Sejalan dengan terus bertambahnya jumlah pengguna Internet, urgensi perlindungan hukum atas data pribadi menjadi semakin penting. Dalam banyak kasus, penting dan perlu untuk menetapkan aturan hukum untuk melindungi data pribadi, terutama karena insiden yang terkait dengan kebocoran data pribadi terjadi dan mengarah pada aktivitas kriminal. Urgensi perlindungan hukum terhadap data pribadi menjadi semakin penting sejalan dengan semakin tingginya angka pemakai telepon seluler dan internet. Banyaknya kasus-kasus terkenal, terutama yang terkait dengan kebocoran data pribadi yang berujung pada penipuan atau kejahatan pornografi, telah memperkuat perdebatan tentang pentingnya ketentuan hukum untuk melindungi data pribadi. Konsep privasi mengacu pada konsep privasi, dan konsep privasi adalah istilah lain yang mengacu pada hak yang perlu dilindungi, yaitu data pribadi sebagai hak yang tidak mengganggu kehidupan pribadi individu.⁶

Teknologi Informasi dan Komunikasi saat ini berkembang dengan cepat dalam berbagai bidang keilmuan.⁷ Kelahiran teknologi AI tidak lepas dari peran yang dimainkan oleh matematikawan Inggris Alan Turing dalam membuat suatu gagasan yaitu sebuah tes untuk memastikan apakah mesin bisa disebut cerdas.⁸ Hasil tes tersebut dinamakan sebagai tes Turing. *Artificial Intelligence* (AI) diajukan oleh Profesor John McCarthy dari Massachusetts Institute of Technology pada Dartmouth Conference 1956. Maksud utama dari adanya kecerdasan buatan adalah untuk mengidentifikasi dan menyerupai proses berpikir manusia dan merancang mesin yang meniru manusia. Dalam hukum Indonesia AI disamakan dengan "Agen Elektronik" karena sifatnya dalam otomatisasi pemrosesan informasi. "Agen Elektronik" Dalam Pasal 1 UU ITE. Pengaturan "Agen Elektronik" dalam rangka transaksi elektronik disebutkan dalam pasal 21 UU ITE. Menurut UU ITE, penyelenggara agen elektronik pada hakekatnya adalah penyelenggara

⁴ Pradana, Agung. "Analisis Statistik pada Dampak Negatif dari Sosial Media Terhadap Perilaku Manusia." *Jurnal of Information Technology and Computer Science* 4 No. 1: (2019), 2.

⁵ Anang, Sugeng Cahyono. "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia." *Jurnal Publiciana Universitas Tulungagung* 9 No. 1: (2016), 1.

⁶ Rosalinda, Elsin Latumahina. "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya". *Jurnal GEMA AKTUALITA* 3 No. 2: (2014), 17.

⁷ Muhajir, Affandi. *Teknologi Informasi dan Komunikasi Dalam Pendidikan* (Jakarta, YNHW, 2018), 7.

⁸ Hani, Subakti. *Artificial Intelligence*. (Bandung, Media Sains Indonesia, 2022), 5.

sistem elektronik. Hal ini disebabkan agen elektronik sebenarnya merupakan salah satu jenis penyelenggara sistem elektronik. Oleh karena itu penyelenggara agen elektronik memiliki hal dan kewajiban yang sama dengan penyelenggara sistem elektronik. Setiap penyelenggara sistem elektronik bertanggung jawab untuk memastikan bahwa sistem yang digunakannya aman, dapat diandalkan dan akurat. Oleh karenanya penyelenggara agen elektronik bertanggung jawab penuh atas setiap dan segala akibat hukum. Tidak menyebabkan kesalahan atau tidak berfungsinya sistem elektronik.

AI tidak diakui sebagai subjek hukum seperti manusia, meskipun faktanya dapat berfungsi serupa dengan kecerdasan manusia. Karena komputer tidak dapat memahami pengetahuan atau niat subjektif, maka perlu untuk fokus pada manusia yang telah mengembangkan atau menyebarkan AI untuk tujuan jahat dan menunjukkan niat jahat. Dengan segala hal yang menimbulkan kerugian bagi pihak lain, dapat dipertanggungjawabkan melalui pihak yang menciptakan dan mengembangkan AI tersebut. Hal ini sejalan dengan apa yang dikatakan oleh *United Nations Commission on International Trade Law (UNCITRAL)* dalam penjelasannya yang menyatakan prinsip umum dalam pasal 12 mendefinisikan bahwa seseorang baik orang perseorangan maupun badan hukum adalah bertanggung jawab atas setiap hal yang dihasilkan oleh mesin. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juncto Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) mengatur teknologi secara umum tetapi tidak membahas secara spesifik mengenai teknologi AI. Selain itu, belum banyak aturan hukum berupa perundang-undangan mengenai penggunaan dan dampak teknologi seperti AI. Permasalahan keamanan dan perlindungan data pribadi pengguna merupakan contoh risiko yang dapat menimbulkan permasalahan mengenai penggunaan dan pemanfaatan AI di Indonesia. Kasus pencurian data pelanggan di salah satu *marketplace* di Indonesia dengan jumlah fantastis pada tahun 2020.⁹ Merupakan salah satu ancaman yang sangat jelas mengenai ancaman AI di masa yang akan datang apabila disalahgunakan oleh pihak yang tidak bertanggung jawab.

3.2. Perlindungan Terhadap Korban Penyalahgunaan Teknik *Deepfake* Terhadap Data Pribadi.

Deepfake adalah bukti bahwa AI dapat memperlihatkan serta memanipulasi video seakan-akan video itu benar dibuat oleh orang di dalam video. Keberadaan *deepfake* awalnya dipersepsikan berbeda oleh komunitas dunia maya. Kemunculannya pertama kali pada tahun 2017 dianggap sebagai hiburan karena *deepfake* sangat populer saat itu untuk memanipulasi video porno. Baru pada tahun 2018 sejumlah *deepfake* politik muncul, menampilkan tokoh-tokoh kunci seperti Nancy Pelosi, Barack Obama, Alexandria Ocasio-Cortez. Munculnya *deepfake* dengan nuansa politik dirasakan oleh komunitas dengan cara yang berbeda dari mereka, masyarakat mulai menganggapnya serius karena dapat berdampak nyata pada masyarakat, seperti ujaran kebencian, pembubaran, konflik, aktivitas kriminal, dan intoleransi. Kasus serupa terjadi di Indonesia di mana Direktorat Tindak Pidana Siber Bareskrim Polri menangani kasus seorang pria yang ditangkap karena karena memposting konten yang menyinggung etnis dan merombak dan menyunting foto Presiden Joko Widodo, pria tersebut juga berniat mengarahkan kebencian

⁹ Kompasiana, 2021, "Kejahatan Pembobolan Sistem dan Pencurian Data (Studi Kasus: E-Commerce)" URL: https://www.kompasiana.com/ulungpriyo3103/5fbb80c18ede480acb2c1dc2/kejahatan-pembobolan-sistem-dan-pencurian-data-studi-kasus-e-commerce?page=5&page_images=2 dikutip pada 12 November 2021.

terhadap orang lain melalui rasisme. Tersangka juga dengan sengaja menunjukkan kebencian atau penghinaan terhadap satu atau lebih kelompok orang Indonesia. Peningkatan kasus tersebut bermula ketika tim patroli siber mendapatkan akun bernama Ahmad Fatihul Alif yang berisi ucapan kebencian dan rasisme. Dengan memanfaatkan dua akun Facebook, yaitu akun Facebook bernama Ahmad Fatihul Alif dan Ilham Al Syahidi, untuk menyebarkan konten ofensif. Munculnya *deepfake* yang disalahgunakan dapat berdampak nyata pada konteks sosial masyarakat, termasuk ujaran kebencian, konflik, perpecahan, peningkatan intoleransi, dan aktivitas kriminal. Penyalahgunaan aplikasi *deepfake* dapat merugikan masyarakat. Jika demikian, penyalahgunaan aplikasi *Deepfake* dapat menjadi kejahatan. Ada korban yang dirugikan dan penyebabnya.

Seiring berjalannya waktu, teknologi ini semakin canggih, meningkatkan hoaks, berita palsu, dan pornografi berbasis *deepfake*. Sebuah foto editan kontroversial tentu akan menimbulkan opini negatif publik. Buatan editan foto *deepfake* terlihat begitu nyata dan sulit dibedakan dari aslinya sehingga bisa menipu masyarakat umum. *Deepfake* dapat disalahgunakan untuk membuat konten negatif, terutama menargetkan selebriti untuk meningkatkan minat publik dalam meneliti konten tersebut. Dengan akses mudah ke aplikasi berbasis *deepfake*, kasus seperti itu dapat berulang terus menerus tanpa tindakan pencegahan apapun. Edit foto dan video secara bebas tanpa batas. Sehingga sangat dibutuhkan adanya peraturan seperti undang-undang dan peraturan yang dapat memberikan aturan yang jelas dan sanksi yang tegas untuk mencegah terulangnya jenis kejahatan yang sama dan untuk mengurangi akibat dan kerugian dari eksploitasi kejahatan *deepfake*. Jika ada penyalahgunaan aplikasi *deepfake* yang bisa merugikan seseorang, maka penyalahgunaan aplikasi *deepfake* bisa menjadi kejahatan. Dengan memenuhi syarat-syarat kriminalisasi seperti perbuatan yang merugikan masyarakat luas, dilakukan secara terus-menerus, adanya reaksi terhadap perbuatan itu, adanya unsur pembuktian, dan bahwa dengan memenuhi segala kriteria yang diperlukan untuk tindakan dapat dikatakan menjadi tindak pidana, dan tergolong menjadi tindakan kriminal pada aplikasi *deepfake* serta memuat cara mengedit foto dan video tergolong kriminal. Maka al tersebut dapat dapat diklasifikasikan sebagai tindak pidana.

Hak atas privasi diakui sebagai hak asasi manusia melalui perlindungan data adalah syarat utama kebebasan pribadi, karena merupakan konsep yang sangat sulit untuk dijelaskan secara definisi. Perlindungan data pribadi merupakan kekuatan pendorong di balik terwujudnya kebebasan politik, intelektual dan agama, termasuk kegiatan pribadi. Hak atas privasi juga dapat dilihat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM) yang di dalam pasal 12 menyatakan tidak dapat seorang pun dapat diganggu secara sewenang-wenang dengan prvasinya, keluarga, rumah atau korespondensinya, atau untuk menyerang kehormatan dan reputasinya. Setiap orang berhak bebas kepada setiap gangguan atau serangan semacam itu. Ketentuan mengenai perlindungan data pribadi dapat ditemukan di dalam pasal Pasal 28 G Ayat (1) UUD 1945 yang menyatakan setiap orang berhak atas perlindungan atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. selain perlindungan konstitusional Indonesia juga tergabung dalam *International Covenant on Civil and Political Rights (ICCPR)* yang disahkan melalui UU Nomor 12 Tahun 2005 yang menjelaskan kepada pemerintah untuk melindungi data pribadi warga negaranya.

Pemerintah Indonesia saat ini telah membuat aturan yang mengatur mengenai hal yang berkaitan dengan data pribadi yang diantaranya terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik sebagaimana yang tertuang dalam pasal

26 Ayat 1 yang menjelaskan pemanfaatan informasi via elektronik yang berkaitan dengan data pribadi harus berdasarkan persetujuan orang yang bersangkutan. Undang – Undang Nomor 10 Tahun 1998 tentang Perbankan Dalam Pasal 40 Ayat (1) menyatakan bahwa “Bank Wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A”. Undang-Undang nomor 23 Tahun 2006 tentang Administrasi Kependudukan menyatakan data pribadi adalah data perorangan yang disimpan, dijaga, dirawat dan dilindungi kerahasiaannya. Peraturan Nomor 36 Tahun 1999 tentang Telekomunikasi, dalam Pasal 42 Ayat (1) menyatakan bahwa organisasi spesialis komunikasi media adalah terikat. merahasiakan data yang dikirim dan diperoleh oleh klien administrasi telekomunikasi melalui organisasi transmisi media atau kemungkinan administrasi telekomunikasi. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia pada Pasal 29 Ayat (1) yang menyatakan bahwa Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik Dalam UU KIP menjelaskan beberapa jenis informasi publik yang disebutkan dalam Pasal 1 (2). Pasal 6 (3) menyatakan: Informasi Publik yang tidak dapat diberikan oleh Badan Publik sebagaimana dimaksud pada ayat (1) adalah: Data yang bisa. membahayakan negara; Data yang berhubungan dengan kepentingan menjaga bisnis dari persaingan bisnis yang tidak wajar; Data yang terhubung dengan hak istimewa individu; Data. berhubungan dengan misteri pekerjaan; serta Informasi Publik disebutkan. belum didominasi atau direkam. Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang dimana Undang-Undang ini bertujuan melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik atau PSE untuk menvegah penyalahgunaan dari individu yang tidak bertanggung jawab. Diharapkan kedepannya dengan disahkannya UU PDP maka semua harus mempunyai teknologi yang dapat harus ditingkatkan agar mampu menahan serangan siber yang elangsung terus-menerus. Juga cepat dalam penanganan maupun pencegahan serangan siber oleh sistemnya masing-masing. Menkominfo menuturkan UU PDP juga turut mengatur institusi perorangan, pribadi, korporasi di dalam negeri maupun global.

Masalah pertama yang hendak diangkat oleh UU PDP ini adalah a) menjawab kebutuhan akan aturan yang komprehensif mengenai perlindungan data pribadi sebagai bagian dari hak asasi manusia. Ini menyeimbangkan pengelolaan data pribadi dengan perlindungan hak dan persepsi subjek data. Pencegahan dan penanganan kebocoran informasi pribadi. Membangun sistem biologi ekonomi yang terkomputerisasi. keamanan melalui perluasan keyakinan sah perusahaan dan kepastian pembeli. Pemerataan dalam aturan PDP global untuk membantu perkembangan moneter terkomputerisasi melalui aliran informasi lintas jalur¹⁰ UU Perlindungan Data Pribadi adalah instrumen yang sah. yang hadir dalam perangkat hukum umum di Indonesia. Kekhawatiran sentral akan. PDP ini adalah a) menjawab kebutuhan akan pedoman yang menjangkau jauh untuk melindungi informasi individu sebagai komponen kebebasan bersama. Keseimbangan dalam administrasi penanganan informasi individu dan jaminan keamanan hak istimewa dan kesadaran subjek informasi. Penghindaran dan penanganan contoh pemutusan informasi individu. Membangun sistem biologis ekonomi terkomputerisasi yang

¹⁰ Henri Subiakto, 2021 “Perlindungan Data Pribadi dan Tantangannya”URL: <https://bappeda.kaltimprov.go.id/storage/data-paparans/September2021/kT1sVHU5rkb1BCP3A2q6.pdf>. dikutip pada 4 Juni 2022.

terlindungi dengan memberikan kepastian yang sah kepada organisasi dan memperluas kepastian pembeli. Keseimbangan dalam PDP global memutuskan yang menjunjung tinggi perkembangan moneter terkomputerisasi melalui aliran informasi lintas-garis. Pasal 27 UU ITE yang biasa ditujukan dalam menangkap pelaku dalam kasus penyebaran informasi, menyatakan bahwa dengan sengaja dan tanpa persetujuan, setiap individu menyebarkan dan juga mengomunikasikan atau berpotensi memberikan data serta arsip elektronik yang isinya bertentangan dengan kebaikan. Setiap orang dengan sengaja dan tanpa hak menyebarkan, mentransmisikan atau memberikan data elektronik dan tambahan catatan elektronik yang mengandung substansi taruhan. Setiap orang yang dengan sengaja dan tanpa hak membubarkan dan juga mengirimkan serta memberikan data elektronik atau laporan yang berpotensi mengandung penghinaan atau berpotensi kritik. Menyebarkan atau berpotensi berkomunikasi serta memberikan data elektronik dan juga arsip yang berisi pemerasan dan juga bahaya bagi siapa saja. Pengaruh inovasi deepfake pada regulasi publik Indonesia terkait dengan jaminan informasi individu tidak sepenuhnya membatasi dengan alasan bahwa adanya pembatasan dalam peraturan perlindungan data pribadi

Di negara Eropa sudah menjalani mengenai perlindungan data pribadi yang mumpuni untuk melindungi data pribadi. Dimana warga negaranya dapat menuntut pemenuhan apa yang disebut "hak untuk dilupakan" (RTBF).¹¹ Mengenai kewenangan ini, menjadi pembahasan pertama dan difokuskan ketika pada tahun 2014 Mario Costeja Gonzalez di Pengadilan Eropa Klaim mencatat masalah dengan Google Spanyol terkait data. dapat diakses dalam dokumen komputerisasi kertas LaVanguardia. Data ini mencakup pemberitahuan penjualan tanah tahun 1998 dan kelanjutannya dengan teknik pengumpulan kewajiban pensiun yang dikelola pemerintah. Akhirnya, kasus tersebut dimenangkan oleh European Court of Justice dan Google Spanyol berkewajiban untuk menghilangkannya. Episode ini menarik pertimbangan banyak individu. Sejak saat itu, minat untuk opsi hak untuk dilupakan telah berkembang. Mengingat informasi publik dari situs Google yang sebenarnya, jumlah koneksi yang dinilai untuk dihapus adalah 1,63 juta¹² Ini merupakan ide kesadaran bahwa hak untuk dilupakan adalah kepunyaan moral yang sangat penting berupa hak moral yang harus dihormati oleh semua lapisan masyarakat dalam pelaksanaan dan penyebarannya. Gugatan ini merupakan tonggak sejarah pemahaman bahwa hak untuk dilupakan adalah hak moral yang sangat penting. Kasus ini menjadi titik awal interpretasi mengenai yang sangat berpengaruh sebagai bentuk dari hak diri pribadi.¹³

Instrumen hukum serupa RTBF telah dijadikan dalam sistem hukum Indonesia, RTBF diatur dalam Pasal 26 ayat (3) UU ITE yang memfokuskan pada pemberian hak kepada individu untuk meminta penghapusan informasi atau data mengenai individu tersebut.¹⁴ Dimana setiap

¹¹ Sayid, Muhammad Rifki Noval. "Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi Penggunaan Teknik Deepfake." *Prosiding Seminar Nasional Penelitian & Pengabdian Kepada Masyarakat*, (2020):5-6.

¹² Balairungpress, 2020, "Hak Untuk Dilupakan di Tengah Keabadian Digital" URL: pada <https://www.balairungpress.com/2020/01/hak-untuk-dilupakan-di-tengah-keabadian-digital/dikutip> 4 Juni 2022

¹³ Hwian, Christianto. "Konsep Hak Untuk Dilupakan Sebagai Pemenuhan Hak Korban Revenge Porn Berdasarkan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik." *Jurnal Mimbar Hukum: Universitas Gadjah Mada* 32 No 2: (2020), 186.

¹⁴ Bernadeta, Erika Noviani. "Analisis Yuridis Mengenai Right To Be Forgotten Sebagai Perlindungan Hak Privasi Ditinjau Dari Undang-Undang Informasi Transaksi Elektronik dan Peraturan Hukum Uni Eropa" *Skripsi: Fakultas Hukum Universitas Katolik Parahyangan* (2018), 45.

penyelenggara sistem elektronik diharapkan untuk menghapus informasi dan elektronik yang berlebihan di bawah pengaruhnya sesuai dengan individu. Pasal UU ITE tentang penghapusan informasi mengenai satu sisi untuk diabaikan seperti Pasal 17 Peraturan Perlindungan Data Umum (GDPR). GDPR adalah panduan perlindungan data mendasar yang digunakan sebagai pedoman. Aturan hukum mengenai teknologi deepfake tidak diatur oleh hukum internasional. Hukum internasional sekarang memberikan fleksibilitas kepada negara-negara untuk menetapkan aturan mereka sendiri mengenai penggunaan teknologi di sektor informasi. Namun, hukum internasional telah melakukan beberapa upaya untuk menyelaraskan aturan tentang masalah ini. Serikat Telekomunikasi. Pasal 1 Konvensi menetapkan tujuan Persatuan Telekomunikasi Internasional dalam bentuk sebagai berikut: a) untuk memelihara dan memperluas kerja sama internasional antara semua Anggota perhimpunan untuk peningkatan dan penggunaan semua jenis telekomunikasi secara rasional, b) untuk menyebarluaskan serta menawarkan bantuan kepada negara-negara berkembang di bidang telekomunikasi dan juga untuk mempromosikan pergerakan sumber daya material dan keuangan yang diperlukan dalam pelaksanaan. c) Mempromosikan pengembangan fasilitas teknis dan pengoperasiannya yang paling efisien dengan tujuan untuk meningkatkan efisiensi layanan telekomunikasi, meningkatkan kegunaannya dan membuatnya sejauh mungkin tersedia untuk umum. d) Untuk mempromosikan perluasan manfaat dari teknologi telekomunikasi baru untuk semua penduduk dunia. e) Mempromosikan penggunaan jasa telekomunikasi dengan tujuan memfasilitasi hubungan damai. f) untuk menyelaraskan tindakan anggota dalam mencapai tujuan tersebut. g) Untuk mempromosikan di tingkat internasional adopsi pendekatan yang lebih luas untuk masalah telekomunikasi dalam ekonomi dan masyarakat informasi global, dengan bekerja sama dengan organisasi antar pemerintah dunia dan regional lainnya dan organisasi non-pemerintah yang peduli dengan telekomunikasi.

Mengacu pada salah satu tujuan Persatuan Telekomunikasi Internasional, butir "g" secara khusus menunjukkan bahwa Konvensi bertujuan untuk mempromosikan adopsi pendekatan yang lebih variatif dilihat dari masalah telekomunikasi dalam kemajuan informasi dan ekonomi dunia yang sedang berkembang. Berkoordinasi dengan asosiasi antar pemerintah dan non-administrasi tentang masalah komunikasi siaran. Hal ini mencerminkan keprihatinan tentang perkembangan teknologi dan kebutuhan untuk memperbarui, melengkapi dan memberikan norma hukum internasional terkait teknologi yang berkelanjutan dan konsisten dengan masyarakat internasional. Mengapa teknologi deepfake membutuhkan regulasi internasional karena Video deepfake dapat menyebabkan keresahan sosial dan memicu teori konspirasi palsu. Deepfake dapat menjadi alat periklanan dan politik dalam hal konflik antar kelompok, penyebaran kata-kata kebencian seperti SARA, dan penyebaran ekstremisme. Ketika deepfake menjadi lebih umum dan berkembang, kontrol yang jelas dan pembatasan hukum menjadi semakin penting. Selain itu, penjahat digital menjadi semakin pintar dalam menemukan kerentanan, terutama karena lebih banyak aplikasi dikirimkan dengan keamanan yang kurang optimal, sehingga masyarakat umum tentang pemahaman digital perlu dididik. Terdapat beberapa hal yang harus diperhatikan mengenai keamanan bagaimana cara menghindari potensi kerugian yang signifikan, mengurangi risiko penyalahgunaan data dan informasi, dan meminimalkan kemungkinan aktivitas kriminal. Selain itu, ada beberapa hal yang dapat melindungi dari pencurian data pribadi, seperti: Waspada hal-hal kecil, seperti membatasi akses orang lain terhadap informasi di perangkat kita. Hapus data atau informasi sesuai kebutuhan. Batasi akses dan batasi akses ke aplikasi telepon.

Kelompok pembelaan global BSA, SoftwareAlliance, mengklaim bentuk untuk melindungi perangkat Anda dari serangan siber adalah dengan memakaiperangkat lunak

resmi Information from BSA individuals, for example, IBM and McAfee detail that online protection dangers are exacerbated by the broad utilization of unlicensed programming in Southeast Asia. Dikatakan juga bahwa sekitar 83 persen perusahaan besar Indonesia saat ini memakai perangkat lunak yang tidak terdaftar. Sejak pandemi Covid-19, mekanisme BSA telah berubah secara dramatis, dengan keamanan siber menjadi fokus utama di kawasan ASEAN.¹⁵ Dengan pemikiran ini, BSA meluncurkan kampanye legalisasi dan perlindungan regional dalam bentuk mengundang orang untuk menggunakan perangkat lunak asli di Indonesia, Vietnam, Thailand dan Filipina. Hasil survei nasional Indeks Literasi Digital Indonesia tergolong moderat, dan saat ini, ketika pengetahuan sumber daya manusia masih lemah, perlindungan kerentanan data pribadi sangat tinggi, terutama dalam menjaga peningkatan aktivitas keamanan siber. ruang digital. Melalui Manajemen Umum Aptika, Kemkominfo telah meluncurkan serangkaian inisiatif untuk meningkatkan keterampilan sumber daya manusia Indonesia, termasuk bermitra dengan platform terkemuka seperti Cisco dan Microsoft untuk menjalankan program beasiswa talenta digital. Pemerintah juga sangat berhati-hati dalam melindungi informasi pribadi semua warga negara melalui program pendidikan digital. Literasi privasi adalah kemampuan memanfaatkan inovasi canggih dan instrumen khusus untuk mendapatkan, menetapkan, mengoordinasikan, memecah, menilai data, membuat informasi baru, berbicara dengan orang lain, dan benar-benar tertarik. Hal ini memiliki arti untuk memperlihatkan kepada masyarakat betapa pentingnya melindungi data pribadi di era digitalisasi kekayaan warga negara Indonesia. Keamanan data pribadi masih jarang dibicarakan di Indonesia. Ketika Internet muncul, kesadaran akan keamanan informasi pribadi seharusnya sudah mulai menyebar. Tapi kenyataannya tidak. Akibatnya sering terjadi penyalahgunaan data dan informasi, dan sulit untuk melacak jumlahnya. Oleh karena itu, menjadi penting untuk mengetahui keamanan data pribadi. Dikarenakan hal ini berkaitan dimana semakin canggih teknologi yang ada, maka juga semakin banyak juga dibutuhkan data dan informasi. Hal pertama yang dapat dilakukan untuk melindungi korban penyalahgunaan data pribadi dengan menggunakan teknologi deepfake adalah masyarakat umum khususnya aparat penegak hukum menyadari keberadaan deepfake abuse sebagai salah satu bentuk kekerasan berbasis online. Kita membutuhkan kerangka hukum yang bukan hanya sekedar melindungi korban, tetapi juga dapat membuat tidak terulangnya kembali. Mekanisme pencegahan, pengobatan dan pemulihan merupakan inti dari kerangka hukum ini. Besar harapan agar pemerintah segera mengambil tindakan dalam upaya meningkatkan kualitas setiap hari tanpa menghentikan perkembangan teknologi.

4. Kesimpulan

Dapat disimpulkan bahwa AI sebenarnya termasuk ke dalam pengertian Agen Elektornik setelah menganalisis ciri-ciri AI dan pengertian Agen Elektronik menurut UU ITE. Artinya setiap komitmen yang sah dan kewajiban yang sah dari Pakar Eletronik terhubung kepada penyedia perangkat AI. AI adalah perangkat sistem elektronik yang dikendalikan entitas (subjek hukum) untuk memproses informasi elektronik secara otomatis. Hal ini menunjukkan bahwa sebagai Agen Elektronik dan penyelenggara sistem elektronik, entitas yang menangani perangkat elektornik tersebut yang bertanggung jawab. Teknologi Deepfake adalah contoh nyata kemajuan dalam kemampuan AI kecerdasan buatan. Terkait dengan penyalahgunaan Teknik Deepfake terhadap data pribadi Dengan memenuhi syarat-syarat kriminalisasi seperti dikarenakan perbuatan itu merugikan masyarakat luas, dan perbuatan itu terus menerus dilakukan, ada reaksi terhadap

¹⁵ Devi, Suherdi. *Peranan Literasi Digital Di Masa Pandemi* (Jakarta, Cattelya Darmaya Fortuna, 2021), 140.

perbuatan itu, dan ada unsur pembuktian, maka perbuatan tersebut dapat menjadi suatu kejahatan. Perlindungan data pribadi telah diatur didalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kemudian sebagai contoh di negara Eropa dikenal dengan istilah *Right to Be Forgotten* (RTBF) dimana setiap warganya dapat menuntut kepatuhan terhadap hak yang ingin dilupakan sehubungan dengan perlindungan data pribadi. Mengenai RTBF telah diadopsi oleh sistem hukum Indonesia. RTBF diatur dalam Pasal 26 Ayat (3) UU ITE. Perlindungan data pribadi adalah tanggung jawab bersama masyarakat, individu, organisasi, dan pemerintah. Tidak mungkin hanya mengandalkan kehati-hatian masyarakat, melainkan peran pemerintah dalam merumuskan kebijakan hukum yang bertujuan memberikan perlindungan kepada masyarakat.

DAFTAR PUSTAKA

Buku:

Devi, Suherdi, *Peranan Literasi Digital Di Masa Pandemi*. Cattelya Darmaya Fortuna (2021):140
Hani, Subakti. *Artificial Intelligence*. Media Sains Indonesia, (2022):5
Muhajir, Affandi. *Teknologi Informasi dan Komunikasi Dalam Pendidikan*. YNHW, (2018):7

Jurnal:

Ayumedia, Kusnadi. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *Jurnal Hukum:Jurnal Penelitian Bidang Hukum Universitas Wijaya Putra* 2.1 (2021): 2.
Anang, Sugeng Cahyono. "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia." *Jurnal Publiciana*. "Universitas Tulungagung 9.1 (2016): 1.
Bernadeta, Erika Noviani. "Analisis Yuridis Mengenai *Right to Be Forgotten* Sebagai Perlindungan Hak Privasi Ditinjau Dari Undang-Undang Informasi Transaksi Elektronik dan Peraturan Hukum Uni Eropa" *Skripsi Hukum: Fakultas Hukum Universitas Katolik Parahyangan* (2018): 45.
Donovan, Typhon Rachmadie. "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016." *Jurnal Recidive*. "Universitas Sebelas Maret 9.2 (2020): 128-129.
Hwian, Christianto. "Konsep Hak Untuk Dilupakan Sebagai Pemenuhan Hak Korban Revenge Porn Berdasarkan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik." *Jurnal Mimbar Hukum*. "Universitas Gadjah Mada 32.2 (2020): 186.
Muhammad, Ariq Abir Jufri. "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi. *Jurnal Hukum Internasional*" *Jurnal Uti Possidetis*. "Universitas Jambi 2.1 (2021)
Muhammad, Na'im Al Jum'ah. "Analisa Keamanan Dan Hukum Untuk Perlindungan Data Privasi." *Jurnal Cyber Security dan Forensik Digital*. "UIN 1.2 (2018)
Natamiharj, Mindoria. "Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN". (2019)
Pradana, Agung. "Analisis Statistik pada Dampak Negatif dari Sosial Media Terhadap Perilaku Manusia." *Juurnal of Information Technology and Computer Science* 4.1 (2019):2
Rosalinda, Elsin Latumahina. "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya". *Jurnal GEMA AKTUALITA* 3.2 (2014): 17.

Sahat, Maruli Tua Situmeang. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Jurnal Sasi.* Universitas Patimura Hukum 27.1 (2021)

Sayid, Muhammad Rifki Noval. "Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi Penggunaan Teknik Deepfake." *Prosiding Seminar Nasional Penelitian & Pengabdian Kepada Masyarakat*, (2020):5-6.

Website:

Angelica Roseanne, 2021, "Deepfake Bagaimana Mendeteksinya." URL: <https://informatika.uc.ac.id/id/2021/05/deepfake-bagaimana-mendeteksinya/>, dikutip pada 6 Juni 2022.

Balairungpress, 2020, "Hak Untuk Dilupakan di Tengah Keabadian Digital" URL: <https://www.balairungpress.com/2020/01/hak-untuk-dilupakan-di-tengah-keabadian-digital/dikutip> dikutip pada 4 Juni 2022.

Cyberthreat.id, 2019, "Jumlah Video Deepfake Meningkat, Mayoritas Untuk Video Porno". URL: <https://cyberthreat.id/read/3280/Jumlah-Video-Deepfake-Meningkat-Mayoritas-untuk-Video-Porno> dikutip pada 6 Juni 2022.

Henri Subiakto, 2021 "Perlindungan Data Pribadi dan Tantangannya" URL: <https://bappeda.kaltimprov.go.id/storage/data-paparans/September2021/kT1sVHU5rkb1BCP3A2q6.pdf> dikutip pada 4 Juni 2022.

Okezone, 2019, "Viral Aplikasi Tukar wajah ZAO Diduga Curi Data Pengguna", URL: <https://techno.okezone.com/read/2019/09/02/207/2099704/viral-aplikasi-tukar-wajah-zao-diduga-curi-data-pengguna>, dikutip pada 6 Juni 2022.

Wbur, 2021 "Perfect Deepfake Tech Could Arrive Sooner Than Expected." URL: www.wbur.org dikutip pada 6 Juni 2022.

Peraturan Perundang-Undangan:

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

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi