DATA BIOMETRIK WAJAH *INFLUENCER* MENURUT HUKUM POSITIF DI INDONESIA[1]

Oleh :
Antonius Stefanus Senduk [2]
Mercy M.M Setlight [3]
Edwin Neil Tinangon [4]

ABSTRAK

Citra wajah *influencer* yang secara rutin diunggah dalam resolusi tinggi ke berbagai *platform* media sosial menjadikannya rentan terhadap penyalahgunaan, termasuk melalui teknologi *deepfake*. Penelitian ini bertujuan untuk menganalisis kedudukan data biometrik wajah *influencer* menurut hukum positif Indonesia serta menilai kecukupan instrumen hukum yang tersedia dalam merespons risiko manipulasi identitas visual berbasis kecerdasan buatan. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil penelitian menunjukkan bahwa data biometrik wajah *influencer* diklasifikasikan sebagai Data Pribadi yang Bersifat Spesifik berdasarkan Pasal 4 ayat (2) huruf b Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), sehingga setiap pemrosesannya mensyaratkan persetujuan eksplisit, *informed*, dan spesifik sebagaimana diatur dalam Pasal 5, Pasal 20, dan Pasal 22 UU PDP, serta kewajiban *Data Protection Impact Assessment* (DPIA) bagi Pengendali Data Pribadi sesuai Pasal 34 UU PDP. Ketentuan ini diperkuat secara komplementer oleh Pasal 12 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta mengenai hak atas potret, serta Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik mengenai larangan manipulasi informasi elektronik. Ketiga instrumen hukum tersebut membentuk perlindungan berlapis (*multi-layer protection*) terhadap identitas visual *influencer*, meskipun unggahan wajah secara sukarela di media sosial tidak dapat ditafsirkan sebagai persetujuan otomatis (*implied consent*) bagi pemrosesan lanjutan oleh pihak ketiga, dan meskipun pedoman teknis operasional mengenai verifikasi consent lintas platform di Indonesia masih belum tersedia secara memadai dibandingkan kerangka kerja Uni Eropa.

Kata Kunci : *data biometrik; wajah influencer; perlindungan data pribadi; deepfake.*

ABSTRACT

An influencer's facial image, routinely uploaded in high resolution across social media platforms, is highly vulnerable to misuse, including through deepfake technology. This study aims to analyze the legal status of an influencer's facial biometric data under Indonesian positive law and to assess the adequacy of existing legal instruments in responding to AI-driven visual identity manipulation. A normative juridical method is employed, using statute, conceptual, and case approaches. The findings show that an influencer's facial biometric data is classified as Specific Personal Data under Article 4(2)(b) of Law Number 27 of 2022 on Personal Data Protection (PDP Law), requiring explicit, informed, and specific consent under Articles 5, 20, and 22, as well as a mandatory Data Protection Impact Assessment (DPIA) for Data Controllers under Article 34. This protection is complemented by Article 12 of the Copyright Law concerning portrait rights and Article 35 of the Electronic Information and Transactions Law prohibiting the manipulation of electronic information. Together, these three legal instruments form a multi-layer protection over an influencer's visual identity, even though voluntary uploads of one's face on social media

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010211
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

cannot be construed as implied consent for further processing by third parties, and even though Indonesia's technical guidance on cross-platform consent verification still lags behind the European Union framework.

Keywords: *biometric data*; *influencer's face*; *personal data protection*; *deepfake*.

A. PENDAHULUAN

Negara Indonesia adalah negara hukum yang menjunjung tinggi perlindungan terhadap Hak Asasi Manusia, termasuk hak atas privasi dan perlindungan diri pribadi sebagaimana dijamin dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.[5] Pengakuan konstitusional ini menjadi landasan lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang secara khusus mengklasifikasikan data biometrik, termasuk citra wajah (*facial image*), sebagai Data Pribadi yang Bersifat Spesifik karena memiliki risiko penyalahgunaan yang jauh lebih tinggi dibandingkan data pribadi pada umumnya.[6]

Kehadiran UU PDP juga tidak dapat dilepaskan dari kewajiban Indonesia untuk menyesuaikan kerangka hukum nasionalnya dengan standar internasional, khususnya *General Data Protection Regulation* (GDPR) Uni Eropa, yang telah lebih dahulu mengatur secara ketat pemrosesan data biometrik sebagai *special category of personal* data pada Pasal 9 GDPR.[7] Sebelum berlakunya UU PDP, pengaturan perlindungan data pribadi di Indonesia tersebar dalam berbagai peraturan sektoral yang tidak saling terintegrasi, termasuk Undang-Undang Informasi dan Transaksi Elektronik, sehingga kehadiran UU PDP sebagai *lex specialis* memberikan unifikasi norma yang sebelumnya tidak dimiliki oleh sistem hukum Indonesia.

Perkembangan *teknologi generative artificial intelligence* telah mendisrupsi tatanan perlindungan hukum yang ada melalui maraknya teknologi *deepfake*, yaitu teknik sintesis citra dan suara manusia berbasis kecerdasan buatan yang mampu menciptakan representasi visual seolah-olah autentik.[8] Teknologi *deepfake* bekerja dengan melatih model *generative adversarial network* (GAN) menggunakan ratusan hingga ribuan citra wajah target untuk menghasilkan rekonstruksi wajah yang secara visual sulit dibedakan dari aslinya, sehingga profesi yang secara struktural menghasilkan volume data wajah beresolusi tinggi dalam jumlah besar sebagaimana lazim dilakukan oleh *influencer* di media sosial secara inheren menjadi kelompok yang paling rentan terhadap eksploitasi teknologi ini dibandingkan individu pada umumnya.

Influencer, sebagai profesi yang secara sukarela dan konsisten mengunggah data biometrik wajah dan suara dalam resolusi tinggi ke berbagai *platform* media sosial, berada pada posisi yang sangat rentan terhadap eksploitasi semacam ini. Kasus pencatutan wajah mantan Menteri Kesehatan Dr. dr. Terawan Agus Putranto, Sp.Rad. melalui iklan obat palsu berbasis *deepfake* pada tahun 2024,[9] serta kasus serupa yang menimpa akademisi dan praktisi bisnis Prof. Rhenald Kasali pada periode 2025–2026,[10] menjadi bukti konkret bahwa kerangka hukum yang ada perlu diuji konsistensinya dalam menjawab persoalan kontemporer ini. Kedua kasus tersebut memiliki pola yang identik: pemanfaatan citra wajah tokoh publik yang telah lebih dahulu

---

[5] Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; lihat juga Putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024; Jimly Asshiddiqie, Konstitusi dan Konstitusionalisme Indonesia (Jakarta: Sinar Grafika, 2021).

[6] Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 angka 1; lihat juga Predderics Hockop Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia," Jurnal Esensi Hukum 6, no. 2 (2024).

[7] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 4 ayat (1) dan ayat (2).

[8] S. Y. Wahyuningtyas, dkk., Pelindungan Data Biometrik dalam Pemrosesan oleh Artificial Intelligence (AI) untuk Teknologi Deepfake (Jakarta: Universitas Katolik Indonesia Atma Jaya, 2025).

[9] ''Kebrutalan Impersonasi Dokter Terawan dalam Iklan Produk Kesehatan Menyesatkan di Facebook dan Instagram," Kompas.com, 31 Maret 2024.

[10] ''Rhenald Kasali Klarifikasi Soal Dirinya Ditahan Polisi dan Dikaitkan Investasi Bodong," Klik Pendidikan, 16 Maret 2026.

tersebar luas secara sah di ruang digital, kemudian direkayasa tanpa persetujuan untuk kepentingan komersial pihak ketiga yang sama sekali tidak terkait dengan subjek data.

Kajian lain juga mencatat bahwa risiko serupa tidak hanya menyasar tokoh publik dengan visibilitas tinggi, tetapi juga meluas pada praktik pemrosesan data biometrik oleh pihak profesional seperti fotografer yang memanfaatkan teknologi *artificial intelligence* tanpa memperoleh persetujuan yang sah dari subjek data, sebuah pola pelanggaran yang secara struktural serupa dengan yang dihadapi *influencer*.[11] Persamaan pola ini memperlihatkan bahwa persoalan pemrosesan data biometrik wajah tanpa persetujuan yang sah bersifat lintas-profesi, dan bukan semata persoalan yang eksklusif dihadapi oleh kalangan *influencer*.

Permasalahan hukum yang muncul terletak pada belum adanya kriteria baku mengenai batas antara persetujuan (*consent*) yang diberikan *influencer* pada saat unggahan awal dengan kebutuhan persetujuan baru ketika data biometrik wajahnya diekstraksi dan direkayasa oleh pihak ketiga untuk tujuan komersial yang berbeda. Kekaburan ini diperparah oleh belum adanya kewajiban hukum yang eksplisit bagi *platform* media sosial untuk menyediakan mekanisme verifikasi *consent* yang terstandardisasi, sehingga tanggung jawab pembuktian persetujuan pada praktiknya dibebankan sepenuhnya kepada subjek data yang haknya dilanggar.

Berdasarkan uraian tersebut, rumusan masalah yang dikaji dalam artikel ini adalah: bagaimana kedudukan hukum data biometrik wajah *influencer* menurut hukum positif di Indonesia, dan sejauh mana instrumen hukum yang tersedia mampu memberikan perlindungan yang efektif terhadap risiko manipulasi berbasis kecerdasan buatan? Artikel ini bertujuan untuk menganalisis kedudukan hukum data biometrik wajah *influencer*, mengidentifikasi instrumen hukum yang relevan dalam memberikan perlindungan terhadapnya, serta menilai kesenjangan implementasi yang masih terbuka dalam praktik penegakan hukum saat ini.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yuridis normatif, yakni penelitian yang dilakukan dengan cara menelaah bahan pustaka atau data sekunder berupa norma hukum yang terdapat dalam peraturan perundang-undangan.[12] Penelitian ini menggunakan tiga pendekatan, yaitu pendekatan perundang-undangan (*statute approach*) terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik; pendekatan konseptual (*conceptual approach*) terhadap konsep persetujuan dan kedaulatan data; serta pendekatan kasus (*case approach*) terhadap kasus *deepfake* yang menimpa tokoh publik.

Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan putusan Mahkamah Konstitusi; bahan hukum sekunder berupa buku teks, jurnal ilmiah, dan hasil penelitian terdahulu; serta bahan hukum tersier berupa kamus hukum dan pemberitaan media massa yang memuat kasus konkret. Ketiga jenis bahan hukum tersebut dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara kualitatif deskriptif dengan metode penalaran deduktif, yakni menarik kesimpulan dari norma hukum yang bersifat umum menuju

[11] Bandingkan dengan G. P. A. Indrayana dan H. Christianto, "Pemrosesan Data Biometrik Melalui Teknologi Artificial Intelligence Oleh Fotografer Tanpa Persetujuan Yang Sah", YUSTISI, Vol. 13, No. 2 (2026), yang mengangkat pola pelanggaran serupa pada konteks profesi lain yang memproses data wajah secara masif.

[12] Jonaedi Effendi dan Johnny Ibrahim, Metode Penelitian Hukum Normatif dan Empiris (Jakarta: Kencana, 2018); Peter Mahmud Marzuki, Pengantar Ilmu Hukum, Edisi Revisi (Jakarta: Kencana, 2011); lihat juga Mercy Maria Magdalena Setlight, dkk., "The Online Loans And Protection Of Users' Personal Data: A Normative Judicial Approach," Pena Justisia: Media Komunikasi dan Kajian Hukum, Vol. 23, No. 1 (2024).

penerapannya pada persoalan konkret pemrosesan data biometrik wajah *influencer*.

C. PEMBAHASAN

Hukum positif tidak hanya terbatas pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai instrumen utama (*lex specialis*), tetapi juga mencakup harmonisasi dengan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Analisis ini didasarkan pada pendekatan *statute approach* sebagaimana dikemukakan oleh Peter Mahmud Marzuki (2011) dan diperkuat oleh teori hierarki norma (*Stufentheorie*) Hans Kelsen yang menempatkan UUD 1945 sebagai *grundnorm*, UU PDP sebagai norma tertinggi di bidang perlindungan data pribadi, serta peraturan pelaksana di bawahnya.

1. Klasifikasi Data Biometrik Wajah sebagai Data Pribadi Spesifik dalam UU PDP

Pasal 4 ayat (1) dan ayat (2) UU PDP membagi Data Pribadi menjadi dua kategori, yaitu Data Pribadi yang bersifat umum dan Data Pribadi yang bersifat spesifik.[13] Data Pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data yang dikombinasikan untuk mengidentifikasi seseorang, sedangkan Data Pribadi yang bersifat spesifik meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lain sesuai ketentuan peraturan perundang-undangan. Data biometrik, termasuk citra wajah yang digunakan untuk pengenalan identitas unik melalui teknologi *facial recognition*, secara eksplisit dimasukkan ke dalam kategori spesifik karena pemrosesannya berpotensi menimbulkan dampak yang lebih besar bagi subjek data, antara lain tindakan diskriminasi dan kerugian yang lebih luas.

Citra wajah influencer yang diunggah secara rutin di platform *Instagram*, *TikTok*, dan *YouTube* dalam resolusi tinggi memenuhi unsur Data Pribadi sebagaimana didefinisikan dalam Pasal 1 angka 1 UU PDP, karena memungkinkan identifikasi unik individu melalui fitur biologis yang bersifat permanen.[14] Berbeda dengan data umum seperti nama atau alamat yang dapat diperbarui sewaktu-waktu, data biometrik wajah tidak dapat diganti apabila terjadi kebocoran, sehingga klasifikasinya sebagai data spesifik berimplikasi pada kewajiban penerapan standar perlindungan yang lebih tinggi, termasuk kewajiban melakukan *Data Protection Impact Assessment* (DPIA) sebelum pemrosesan dilakukan sebagaimana diatur dalam Pasal 34 UU PDP.[15]

Karakteristik permanen dan tidak dapat diperbarui (*non-revocable*) inilah yang membedakan urgensi perlindungan data biometrik dari data pribadi pada umumnya. Apabila kata sandi atau nomor rekening dapat diganti setelah terjadi kebocoran, wajah seseorang tidak dapat digantikan sepanjang hidupnya, sehingga sekali data biometrik wajah bocor atau disalahgunakan untuk melatih model *deepfake*, risiko yang timbul bersifat permanen dan berkelanjutan (*perpetual risk*) terhadap subjek data.[16] Prinsip inilah yang menjadi rasionalisasi normatif di balik penempatan data biometrik pada kategori data spesifik dalam Pasal 4 ayat (2) UU PDP, dan sekaligus menjadi argumen bahwa standar persetujuan bagi pemrosesan data biometrik wajah *influencer* semestinya lebih ketat dibandingkan standar persetujuan bagi pemrosesan data pribadi umum seperti nama pengguna atau alamat surel.

---

[13] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 4 ayat (1) dan ayat (2).

[14] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 angka 1; lihat juga Predderics Hockop Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia," Jurnal Esensi Hukum, Vol. 6, No. 2 (2024).

[15] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 34.

[16] Bandingkan konsep non-revocable biometric identifier dalam Wahyuningtyas, dkk., Op. Cit., yang menekankan bahwa sifat permanen data biometrik menuntut standar kehati-hatian pemrosesan yang jauh lebih tinggi dibandingkan data pribadi umum.

2. Persyaratan Persetujuan (*Consent*) yang Eksplisit, *Informed*, dan Spesifik

Pasal 5 UU PDP menjamin hak Subjek Data Pribadi untuk memperoleh informasi yang jelas mengenai identitas Pengendali Data Pribadi, dasar kepentingan hukum pemrosesan, dan tujuan penggunaan data. Pasal 20 ayat (2) huruf a jo. Pasal 22 ayat (1) UU PDP mensyaratkan bahwa persetujuan harus diberikan secara eksplisit, melalui cara tertulis atau terekam, untuk satu atau beberapa tujuan tertentu yang telah disampaikan secara jelas.[17] Persetujuan yang sah pada hakikatnya harus memenuhi unsur *freely given*, *specific*, *informed*, dan *unambiguous*, yang secara sistematis dapat ditafsirkan dari norma-norma UU PDP tersebut.

Keempat unsur ini sejalan dengan konsepsi *lawfulness of processing* dalam *Article* 6 GDPR, yang telah lebih dahulu menetapkan standar serupa di tingkat internasional.[18] Kesamaan struktur norma ini memperlihatkan bahwa pembentuk undang-undang Indonesia secara sadar mengadopsi standar internasional dalam merumuskan syarat sahnya persetujuan, sehingga interpretasi terhadap unsur eksplisit, *informed*, dan spesifik dalam UU PDP dapat memperoleh pembanding yang relevan dari praktik penerapan GDPR di Uni Eropa, khususnya dalam menilai apakah suatu bentuk persetujuan telah memenuhi standar yang dipersyaratkan.

Unggahan foto atau video wajah oleh *influencer* untuk tujuan *personal branding* atau *endorsement* tidak dapat ditafsirkan secara otomatis sebagai persetujuan bagi pemrosesan lebih lanjut berupa ekstraksi data biometrik untuk teknologi *deepfake* atau penggunaan komersial oleh pihak ketiga. Penafsiran bahwa unggahan di media sosial merupakan *implied consent* atau *blanket consent* bertentangan dengan asas pembatasan tujuan (*purpose limitation*) dan prinsip minimisasi data yang menjadi jiwa Pasal 16 ayat (2) huruf a dan b UU PDP.[19] Oleh karena itu, setiap pemrosesan data biometrik wajah *influencer* untuk tujuan yang berbeda dari tujuan awal unggahan tetap memerlukan persetujuan baru yang *informed* dan spesifik.

Prinsip *purpose limitation* ini secara konseptual berarti bahwa persetujuan bersifat kontekstual dan terikat tujuan (*context-bound*), bukan persetujuan yang bersifat umum dan berlaku untuk seluruh bentuk pemrosesan selanjutnya. Dengan demikian, ketika sebuah citra wajah *influencer* yang semula diunggah untuk kepentingan promosi produk kecantikan kemudian diekstraksi oleh pihak ketiga untuk melatih model *deepfake* yang digunakan dalam iklan obat-obatan yang sama sekali tidak terafiliasi dengan *influencer* tersebut, telah terjadi pergeseran tujuan pemrosesan (*purpose creep*) yang secara normatif membatalkan keabsahan sandaran hukum berupa persetujuan awal, sehingga pemrosesan lanjutan tersebut kehilangan dasar hukumnya sama sekali.

3. Kewajiban Pengendali Data Pribadi (*Platform* dan *Brand*) serta *Data Protection Impact Assessment (DPIA)*

Pasal 28 hingga Pasal 33 UU PDP mengatur kewajiban Pengendali dan Prosesor Data Pribadi untuk menerapkan prinsip akuntabilitas, mencakup penerapan langkah teknis dan organisasional yang memadai, pencatatan kegiatan pemrosesan, serta pemberitahuan pelanggaran data dalam waktu 72 jam. Platform media sosial dan brand yang memanfaatkan wajah *influencer* untuk kampanye pemasaran berkedudukan sebagai Pengendali Data Pribadi apabila mereka menentukan tujuan dan cara pemrosesan, sehingga wajib memastikan bahwa persetujuan yang diperoleh memenuhi standar eksplisit, *informed*, dan spesifik. Kegagalan memenuhi

[17] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 5, Pasal 20 ayat (2) huruf a, dan Pasal 22 ayat (1).

[18] Article 6 paragraph (1) GDPR ke dalam Pasal 20 Ayat (2) UU PDP, sebagaimana diuraikan dalam "Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022", yang mencatat bahwa penempatan syarat sah pemrosesan data pribadi dalam UU PDP mengikuti urutan yang sama dengan GDPR.

[19] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 16 huruf a dan b; Wahyudi Djafar, Perlindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya (Jakarta: ELSAM, 2019).

kewajiban ini dapat berujung pada sanksi administratif berupa denda hingga 2% dari pendapatan tahunan sebagaimana diatur dalam Pasal 57 UU PDP.[20]

Kewajiban akuntabilitas ini semakin krusial mengingat karakteristik ekosistem influencer marketing yang melibatkan banyak pihak dalam satu rantai pemrosesan data: agensi manajemen talenta, *platform* media sosial, *brand* pengiklan, hingga pihak ketiga penyedia teknologi pengenalan wajah untuk kepentingan analitik kampanye.[21] Dalam rantai pemrosesan yang panjang dan multipihak semacam ini, kejelasan mengenai pihak mana yang berkedudukan sebagai Pengendali Data dan karenanya memikul tanggung jawab hukum utama menjadi krusial, karena tanpa kejelasan tersebut, subjek data (*influencer*) akan kesulitan menentukan pihak mana yang dapat dimintai pertanggungjawaban ketika terjadi pemrosesan data biometrik wajahnya secara melawan hukum.

Kewajiban melakukan DPIA sebagaimana diatur Pasal 34 UU PDP idealnya berfungsi sebagai instrumen mitigasi risiko preventif, yang mewajibkan Pengendali Data untuk mengidentifikasi dan menilai potensi dampak pemrosesan data spesifik sebelum pemrosesan dilakukan, termasuk menilai risiko penyalahgunaan data biometrik wajah untuk tujuan *deepfake*. Namun demikian, UU PDP maupun peraturan pelaksananya belum mengatur secara rinci format, parameter penilaian risiko, maupun mekanisme verifikasi independen atas hasil DPIA yang disusun oleh Pengendali Data, sehingga penerapannya dalam praktik industri periklanan digital yang melibatkan *influencer* masih sangat bergantung pada itikad baik masing-masing pelaku usaha.

4. Harmonisasi dengan UU Hak Cipta dan UU ITE: Larangan Manipulasi dan Penggunaan Komersial Tanpa Izin

Perlindungan data biometrik wajah *influencer* tidak berdiri sendiri dalam UU PDP, melainkan saling melengkapi dengan Pasal 12 ayat (1) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, yang melarang penggunaan secara komersial atas potret seseorang tanpa persetujuan tertulis dari orang yang dipotret.[22] Ketentuan ini memberikan perlindungan tambahan berupa hak moral dan hak ekonomi atas potret yang melekat pada *influencer* sebagai subjek potret.

Konstruksi hukum ini menunjukkan bahwa data biometrik wajah *influencer* sesungguhnya dilindungi oleh dua rezim hukum yang berbeda paradigma sekaligus: rezim hukum privasi dan pelindungan data pribadi yang berorientasi pada kontrol subjek data atas informasi dirinya, serta rezim hukum kekayaan intelektual yang berorientasi pada perlindungan nilai ekonomi dan moral atas representasi visual seseorang. Kedua rezim ini tidak saling meniadakan, melainkan saling melengkapi (*mutually reinforcing*), karena pelanggaran atas data biometrik wajah melalui *deepfake* pada praktiknya sekaligus melanggar hak atas privasi data pribadi dan hak atas potret sebagai bagian dari hak cipta.

Selain itu, Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024 melarang setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, atau penghilangan Informasi Elektronik dengan maksud agar informasi tersebut dianggap seolah-olah autentik.[23] *Deepfake* yang memanipulasi wajah *influencer* untuk kepentingan komersial tanpa persetujuan tertulis dengan demikian merupakan pelanggaran ganda terhadap UU Hak Cipta dan UU ITE sekaligus, dengan ancaman pidana

[20] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 28 sampai dengan Pasal 33.
[21] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 57.
[22] Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, Pasal 12 ayat (1).
[23] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 35.

penjara hingga 12 tahun berdasarkan Pasal 51 ayat (1) UU ITE.[24] Harmonisasi ketiga instrumen hukum ini menciptakan perlindungan berlapis (*multi-layer protection*) bagi *influencer*, meskipun dalam praktiknya pedoman teknis operasional mengenai verifikasi *consent* lintas *platform* masih belum tersedia secara memadai.[25]

5. Kesenjangan Implementasi dan Perbandingan dengan Kerangka Uni Eropa

Meskipun kerangka norma sebagaimana diuraikan pada subbab-subbab sebelumnya secara tekstual sudah memadai, kesenjangan (gap) terbesar terletak pada tataran implementasi, bukan pada tataran norma. Uni Eropa melalui GDPR telah dilengkapi oleh regulasi turunan yang lebih teknis, termasuk pedoman *European Data Protection Board* mengenai penerapan *facial recognition* dan kewajiban *privacy by design*, yang mewajibkan pertimbangan perlindungan data pribadi dilakukan sejak tahap perancangan sistem, bukan sebagai pertimbangan tambahan setelah sistem beroperasi. UU PDP Indonesia belum memiliki padanan yang setara bagi prinsip *privacy by design* tersebut secara eksplisit dalam batang tubuhnya, sehingga penerapannya masih bergantung pada penafsiran ekstensif terhadap kewajiban akuntabilitas Pengendali Data dalam Pasal 28 hingga Pasal 33 UU PDP.

Kesenjangan implementasi lain tampak pada belum adanya lembaga pengawas independen yang secara khusus berwenang menerbitkan pedoman teknis (*technical guidance*) mengenai standar minimum verifikasi *consent* untuk pemrosesan data biometrik lintas *platform*, sebagaimana dijalankan oleh otoritas pengawas data pribadi di berbagai negara anggota Uni Eropa. Ketiadaan lembaga dengan kewenangan serupa di Indonesia menyebabkan interpretasi terhadap unsur eksplisit, *informed*, dan spesifik dalam Pasal 20 dan Pasal 22 UU PDP masih bersifat kasuistis dan bergantung pada penafsiran hakim ketika sengketa diajukan ke pengadilan, alih-alih dipandu oleh pedoman administratif yang bersifat preventif.

Kesenjangan ini juga tercermin dari belum adanya kewajiban hukum yang eksplisit bagi *platform* media sosial untuk menerapkan *watermarking* otomatis atau pelabelan konten hasil kecerdasan buatan (*AI-generated content labeling*), sebuah langkah yang telah mulai diwajibkan di beberapa yurisdiksi lain sebagai instrumen deteksi dini konten *deepfake*.[26] Tanpa kewajiban pelabelan semacam ini, beban pembuktian bahwa suatu konten merupakan hasil manipulasi *deepfake* sepenuhnya berada di pihak korban, yang pada praktiknya kerap tidak memiliki akses maupun kemampuan teknis untuk melakukan forensik digital secara mandiri.

6. Tanggung Jawab Perdata dan Mekanisme Pemulihan bagi Korban

Selain jalur administratif dan pidana yang telah diuraikan pada subbab sebelumnya, Pasal 12 UU PDP membuka jalur tanggung jawab perdata bagi subjek data yang dirugikan akibat pemrosesan data biometrik wajahnya secara melawan hukum, dengan hak untuk mengajukan gugatan dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi.[27] Jalur perdata ini memiliki karakteristik yang berbeda dari jalur pidana maupun administratif; pembuktian dilakukan dengan standar keseimbangan kemungkinan (*preponderance of evidence*), bukan pembuktian di luar keraguan yang wajar (*beyond reasonable doubt*) sebagaimana berlaku dalam hukum pidana, sehingga secara teoretis lebih mudah diakses oleh korban perorangan dibandingkan

[24] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 11 Tahun 2008, Pasal 51 ayat (1).

[25] Anita Firdausi, dkk., "Tinjauan Etis dan Hukum terhadap Perlindungan Data Pribadi di Tengah Maraknya Konten Deepfake di Media Sosial," Causa: Jurnal Hukum dan Kewarganegaraan, Vol. 12, No. 5 (2025); Chiquita Thefirstly Noerman, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," Jurnal USM Law Review, Vol. 7, No. 2 (2024).

[26] Chiquita Thefirstly Noerman, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara", Jurnal USM Law Review, Vol. 7, No. 2 (2024).

proses pidana yang bergantung pada inisiatif penegak hukum.

Meskipun demikian, tantangan praktis dalam mengajukan gugatan perdata atas pelanggaran data biometrik wajah melalui *deepfake* terletak pada kesulitan pembuktian rantai kausalitas, yakni membuktikan bahwa citra wajah yang digunakan dalam konten *deepfake* benar berasal dari data yang diunggah korban tanpa persetujuan lanjutan, dan bukan dari sumber lain yang secara sah telah diberikan izin. Kesulitan pembuktian semacam ini menegaskan kembali pentingnya kewajiban pencatatan kegiatan pemrosesan (*records of processing activities*) oleh Pengendali Data sebagaimana diatur Pasal 28 hingga Pasal 33 UU PDP, karena catatan tersebut pada praktiknya menjadi alat bukti utama bagi korban dalam mengonstruksi rantai kausalitas pemrosesan data biometrik wajahnya.

Perbandingan dengan praktik di Uni Eropa menunjukkan bahwa GDPR menyediakan hak atas kompensasi (*right to compensation*) berdasarkan *Article* 82, yang memungkinkan subjek data mengajukan klaim baik terhadap Pengendali Data maupun Prosesor Data secara tanggung renteng (*joint and several liability*) apabila keduanya terlibat dalam pemrosesan yang melanggar hukum.[28] UU PDP Indonesia belum secara eksplisit merumuskan konstruksi tanggung jawab tanggung renteng semacam ini antara Pengendali dan Prosesor Data, sehingga dalam kasus *deepfake* yang melibatkan rantai pemrosesan panjang mulai dari *platform* media sosial, penyedia teknologi kecerdasan buatan, hingga *brand* pengiklan korban berpotensi menghadapi kesulitan tambahan dalam menentukan pihak mana yang harus digugat terlebih dahulu, atau apakah seluruh pihak dalam rantai tersebut dapat digugat secara bersama-sama.

Kekosongan norma mengenai tanggung jawab tanggung renteng ini menjadi salah satu titik yang perlu mendapat perhatian pembentuk kebijakan ke depan, mengingat karakteristik ekosistem digital yang melibatkan banyak pihak dalam satu rantai pemrosesan data biometrik wajah *influencer*. Tanpa kejelasan konstruksi tanggung jawab tersebut, perlindungan hukum yang secara normatif telah berlapis melalui UU PDP, UU Hak Cipta, dan UU ITE berisiko kehilangan daya cengkeramnya dalam praktik penegakan hukum di pengadilan, karena korban akan dihadapkan pada beban prosedural tambahan untuk mengidentifikasi dan menggugat setiap pihak dalam rantai pemrosesan secara terpisah.

D. Penutup

1. Kesimpulan

Data biometrik wajah *influencer* diklasifikasikan secara rigid sebagai Data Pribadi yang Bersifat Spesifik berdasarkan Pasal 4 ayat (2) huruf b UU PDP, sehingga setiap pemrosesannya wajib bersandar pada persetujuan tertulis yang eksplisit, *informed*, dan spesifik sesuai Pasal 5, Pasal 20, dan Pasal 22 UU PDP, disertai kewajiban *Data Protection Impact Assessment* bagi Pengendali Data Pribadi menurut Pasal 34 UU PDP. Unggahan wajah secara sukarela di media sosial untuk tujuan personal branding tidak dapat ditafsirkan sebagai persetujuan otomatis (*implied consent*) bagi pemrosesan lanjutan yang berbeda tujuan, sejalan dengan asas pembatasan tujuan yang menjadi jiwa UU PDP.

Perlindungan ini terintegrasi secara komplementer dengan Pasal 12 UU Hak Cipta mengenai hak atas potret serta Pasal 35 UU ITE mengenai larangan manipulasi informasi elektronik, sehingga ketiganya membentuk instrumen pelindungan hukum yang bersifat preventif maupun represif atas identitas visual *influencer* di ruang digital. Meskipun demikian, kerangka norma yang secara tekstual sudah memadai ini masih dihadapkan pada kesenjangan implementasi yang signifikan, khususnya ketiadaan pedoman teknis operasional mengenai verifikasi *consent* lintas *platform*, ketiadaan kewajiban *privacy by design* yang eksplisit, dan ketiadaan kewajiban pelabelan konten hasil kecerdasan buatan, yang menjadikan perlindungan hukum bagi data biometrik wajah *influencer* di Indonesia secara normatif berlapis namun secara implementatif masih rentan terhadap celah penegakan.

2. Saran

Disarankan agar pemerintah segera menyusun peraturan pelaksana yang secara teknis mengatur tata cara verifikasi *consent* lintas *platform* serta kewajiban *watermarking* dan pelabelan konten hasil kecerdasan buatan, guna menutup kekosongan norma teknis yang masih terbuka dalam praktik penegakan hukum saat ini. Disarankan pula agar lembaga yang berwenang mengawasi pelaksanaan UU PDP menerbitkan pedoman teknis (*technical guidance*) mengenai standar minimum penilaian *Data Protection Impact Assessment* bagi pelaku usaha yang memproses data biometrik wajah untuk kepentingan komersial, termasuk kewajiban *privacy by design* bagi *platform* media sosial dan agensi manajemen talenta yang menjadi Pengendali Data dalam ekosistem *influencer* marketing di Indonesia.

DAFTAR PUSTAKA

Asshiddiqie, Jimly. Konstitusi dan Konstitusionalisme Indonesia. Jakarta: Sinar Grafika, 2021.

Budhijanto, Danrivanto. Hukum Pelindungan Data Pribadi & Data Nasional. Bandung: Logoz Publishing, 2024.

Djafar, Wahyudi. Perlindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya. Jakarta: ELSAM, 2019.

Effendi, Jonaedi, dan Johnny Ibrahim. Metode Penelitian Hukum Normatif dan Empiris. Jakarta: Kencana, 2018.

Firdausi, Anita, dkk. "Tinjauan Etis dan Hukum terhadap Perlindungan Data Pribadi di Tengah Maraknya Konten *Deepfake* di Media Sosial". Causa: Jurnal Hukum dan Kewarganegaraan, Vol. 12, No. 5, 2025.

Indrayana, G. P. A., dan H. Christianto. "Pemrosesan Data Biometrik Melalui Teknologi *Artificial Intelligence* Oleh Fotografer Tanpa Persetujuan Yang Sah". YUSTISI, Vol. 13, No. 2, 2026.

"Kebrutalan Impersonasi Dokter Terawan dalam Iklan Produk Kesehatan Menyesatkan di *Facebook* dan *Instagram*". Kompas.com, 31 Maret 2024.

"Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022". Jurnal Digital Kementerian Komunikasi dan Digital.

Marzuki, Peter Mahmud. Pengantar Ilmu Hukum, Edisi Revisi. Jakarta: Kencana, 2011.

Noerman, Chiquita Thefirstly. "Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara". Jurnal USM Law Review, Vol. 7, No. 2, 2024.

"Rhenald Kasali Klarifikasi Soal Dirinya Ditahan Polisi dan Dikaitkan Investasi Bodong". Klik Pendidikan, 16 Maret 2026.

Setlight, Mercy Maria Magdalena, dkk. "*The Online Loans And Protection Of Users' Personal Data: A Normative Judicial Approach*". Pena Justisia: Media Komunikasi dan Kajian Hukum, Vol. 23, No. 1, 2024.

Simanjuntak, Predderics Hockop. "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia". Jurnal Esensi Hukum, Vol. 6, No. 2, 2024.

Wahyuningtyas, S. Y., dkk. Pelindungan Data Biometrik dalam Pemrosesan oleh *Artificial Intelligence* (AI) untuk Teknologi *Deepfake*. Jakarta: Universitas Katolik Indonesia Atma Jaya, 2025.

Putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

General Data Protection Regulation (EU) 2016/679.