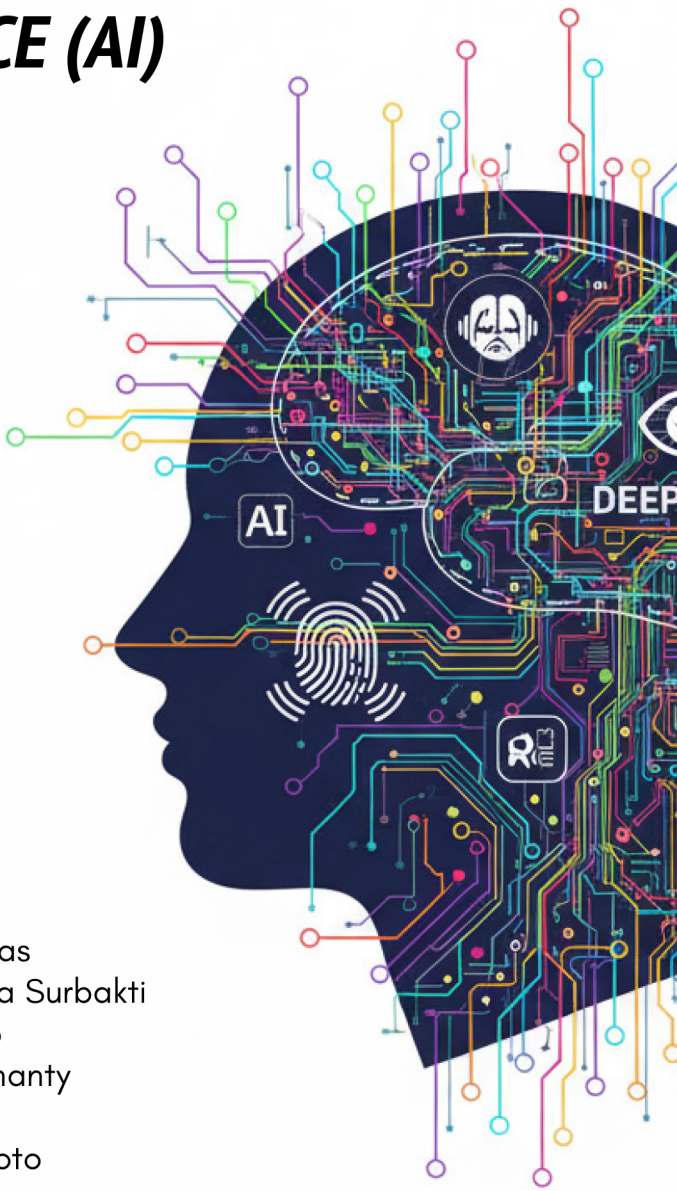
PELINDUNGAN DATA BIOMETRIK DALAM PEMROSESAN OLEH ***ARTIFICIAL INTELLIGENCE (AI)*** UNTUK TEKNOLOGI ***DEEPFAKE***



Disusun oleh

Sih Yuliana Wahyuningtyas
Feliks Prasepta Sejahtera Surbakti
Stephen Aprius Sutresno
Kalistazaira Audriendiamanty
Petrus Dapet
Teresa Kaena Dharmanyoto

PELINDUNGAN DATA BIOMETRIK DALAM PEMROSESAN OLEH ***ARTIFICIAL INTELLIGENCE (AI)*** UNTUK TEKNOLOGI ***DEEPFAKE***

Undang-Undang Republik Indonesia
Nomor 28 Tahun 2014 tentang Hak Cipta

Sanksi Pelanggaran
Pasal 113:

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp 100.000.000 (seratus juta rupiah).

2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (l) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

PELINDUNGAN DATA BIOMETRIK DALAM PEMROSESAN OLEH *ARTIFICIAL INTELLIGENCE (AI)* UNTUK TEKNOLOGI *DEEPFAKE*

Disusun oleh

Sih Yuliana Wahyuningtyas
Feliks Prasepta Sejahtera Surbakti
Stephen Aprius Sutresno
Kalistazaira Audriendiamanty
Petrus Dapet
Teresa Kaena Dharmanyoto

Penerbit ATMA JAYA

Pelindungan Data Biometrik dalam Pemrosesan oleh *Artificial Intelligence* (AI) Untuk Teknologi *Deepfake*

Penerbit Universitas Katolik Indonesia Atma Jaya
Anggota IKAPI–Ikatan Penerbit Indonesia–Jakarta
Anggota APPTI–Afiliasi Penerbit Perguruan Tinggi Indonesia

Penerbit Universitas Katolik Indonesia Atma Jaya
Jl. Jend. Sudirman Kav. 51
Jakarta 12930 Indonesia
Phone : (021) 5703306 psw. 631
E-mail : penerbit@atmajaya.ac.id
Website : http://www.atmajaya.ac.id

Cetakan Pertama, Desember 2025

Penulis : Sih Yuliana Wahyuningtyas
Feliks Prasepta Sejahtera Surbakti
Stephen Aprius Sutresno
Kalistazaira Audriendiamanty
Petrus Dapet
Teresa Kaena Dharmanyoto

Tata Letak : Adi Yuwono
Layout Sampul : Adi Yuwono *(image cover by Gemini AI)*

Pelindungan Data Biometrik dalam Pemrosesan oleh *Artificial Intelligence* (AI) Untuk Teknologi *Deepfake*
Jakarta: Penerbit Universitas Katolik Indonesia Atma Jaya, 2025
x + 66 hlm.; 150 x 230 mm

ISBN: 978-634-7009-55-5
ISBN Digital: 978-634-7009-56-2 (PDF)

Sumber Pendanaan dan *Acknowledgement*

Penelitian hingga penulisan *White Paper ini* sebagai luarannya merupakan program penelitian berjudul "Pelindungan Data Biometrik dalam Pemrosesan oleh *Artificial Intelligence* (AI) untuk Teknologi *Deepfake*" yang merupakan penelitian yang didanai oleh Direktorat Penelitian dan Pengabdian kepada Masyarakat (DPPM) Direktorat Jenderal Riset dan Pengembangan - Kementerian Pendidikan Tinggi Sains dan Teknologi tahun anggaran 2025 ("Hibah DPPM 2025") untuk Penelitian Dasar dengan Skema Penelitian Fundamental Reguler. Tim Peneliti menyampaikan terima kasih kepada DPPM atas bantuan pendanaan yang diberikan sehingga penelitian dapat berlangsung dan menghasilkan luaran sebagai kontribusi akademik untuk pengembangan keilmuan.

Tim Peneliti menyampaikan pula terima kasih kepada para Narasumber dalam serangkaian kegiatan FGD yang diselenggarakan dalam penelitian ini atas semua masukan yang tidak ternilai harganya.

KATA PENGANTAR

Pemrosesan data pribadi yang semakin masif dalam era digital telah menimbulkan kebutuhan untuk pelindungan hukum yang komprehensif, spesifik, dan memadai bagi subyek data. Di Indonesia, dengan diberlakukannya Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), diharapkan akan adanya payung hukum untuk kerangka regulasi yang mumpuni dan berfungsi dengan baik untuk melindungi hak-hak subyek data. Namun demikian, untuk terpenuhinya harapan tersebut, masih perlu ditempuh berbagai upaya termasuka mengidentifikasi kebutuhan-kebutuhan spesifik untuk pelindungan data pribadi dan implementasi mekanisme pelindungannya. Pada saat White Paper ini disusun, Pemerintah masih menjalankan proses untuk penyusunan Peraturan Pemerintah untuk pelindungan data pribadi sebagai aturan turunan dari UU PDP.

Salah satu aspek krusial yang perlu mendapatkan perhatian adalah pelindungan terhadap data biometrik. Dalam UU PDP, data biometrik dikategorikan sebagai salah satu jenis dari data spesifik yang membutuhkan pelindungan khusus untuk pemrosesannya.

Dengan perkembangan teknologi yang semakin pesat, data biometrik semakin banyak digunakan, utamanya untuk tujuan otorisasi, otentikasi, dan verifikasi, karena banyaknya keunggulan dibandingkan dengan otorisasi, otentikasi, dan verifikasi dengan cara tradisional. Keunikan data biometrik merupakan salah satu keterandalan akurasi yang sering dikemukakan. Namun demikian, karena itulah pula pemrosesan data biometrik mengandung risiko yang sangat tinggi bagi keamanan dan privasi. Dalam konteks itulah, Tim Peneliti melakukan penelitian ini, dengan maksud untuk dapat menjawab sejumlah pertanyaan kritis terkait upaya untuk memastikan kendali subyek data atas data biometriknya dalam pemrosesan data. Sebagai fokus yang membatasi ruang lingkup penelitian, analisis atas pelindungan data biometrik dilakukan dalam implementasinya untuk teknologi deepfake yang saat ini semakin masif dan progresif digunakan, yang dalam implementasinya juga menimbulkan banyak persoalan hukum.

Dalam konteks penyusunan kebijakan dan regulasi, salah satu pendekatan yang dapat dipertimbangkan adalah penyusunan kebijakan dan regulasi yang didasarkan pada identifikasi kebutuhan, identifikasi risiko, identifikasi mitigasi atas risiko, dan identifikasi dampak kerugian. Pendekatan semacam ini menjadi penting untuk dapat tersusunnya kebijakan dan regulasi yang menjawab persoalan.

Penelitian ini dilakukan dengan metode yuridis normatif dengan menggunakan studi pustaka *(library research)* yang didukung dengan *forum group discussions* dengan para pemangku kepentingan untuk memperoleh data. Analisis data dilakukan secara kualitatif. *White Paper* ini disusun sebagai hasil dari kegiatan penelitian dan sebagai upaya untuk memberikan kontribusi guna penyusunan kebijakan dan regulasi yang relevan mengenai pelindungan data biometrik. Penelitian dilakukan pelaksanaan program penelitian tahun anggaran 2025 dari Direktorat Penelitian dan Pengabdian kepada Masyarakat (DPPM) Direktorat Jenderal Riset dan Pengembangan - Kementerian Pendidikan Tinggi Sains dan Teknologi (“Hibah DPPM 2025“) oleh Universitas Katolik Indonesia Atma Jaya.

Limpah terima kasih, kami haturkan kepada para Narasunber dalam sejumlah *Forum Group Discussion* (FGD) yang kami selenggarakan untuk mendapatkan masukan, pandangan, dan koreksi. Segala kekurangan dalam naskah ini semata-mata merupakan tanggung jawab kami, Tim Peneliti.

Semoga White Paper ini dapat menjadi bahan rekomendasi yang bermanfaat bagi para pemangku kepentingan, baik penyusun kebijakan dan regulasi, industri, *Non-Governmental Organization* (NGO), lembaga penelitian dan advokasi, akademisi maupun masyarakat luas khususnya individu sebagai subyek data.

Jakarta, 15 November 2025
Tim Peneliti

DAFTAR ISI

BAB 4

BAB 5

BAB 6

BAB 7

BAB 8

BAB
1

PENDAHULUAN

Fenomena *deepfake* merupakan salah satu perkembangan paling menonjol dari revolusi kecerdasan buatan (*Artificial Intelligence*/AI) dalam dekade terakhir. Istilah ini berasal dari gabungan kata deep learning dan fake, yang merujuk pada praktik memanipulasi konten visual maupun audio menggunakan algoritma pembelajaran mendalam (deep learning) untuk menciptakan hasil yang tampak nyata (Kietzmann et al., 2020). Teknologi ini erat kaitannya dengan generative adversarial networks (GANs), suatu model pembelajaran mesin yang diperkenalkan oleh Ian Goodfellow pada tahun 2014. GANs bekerja dengan dua jaringan saraf tiruan yang berkompetisi: generator yang berusaha menciptakan konten palsu yang realistis, dan discriminator yang berusaha membedakan mana konten asli dan mana palsu. Persaingan antara keduanya menghasilkan keluaran yang semakin sulit dibedakan dari kenyataan (Goodfellow et al., 2014).

Pada awalnya, teknologi *deepfake* dipandang sebagai inovasi kreatif dengan potensi luar biasa dalam berbagai bidang. Industri hiburan, misalnya, melihat peluang untuk melakukan *visual effects* yang lebih murah dan realistis dibandingkan teknik tradisional (Bodini et al., 2024). Dalam dunia film, teknologi ini dapat digunakan untuk "menghidupkan kembali" aktor yang telah meninggal atau merekonstruksi tokoh sejarah. Dalam pendidikan, *deepfake* berpotensi menghadirkan metode pembelajaran interaktif dengan menciptakan simulasi tokoh penting, atau menyajikan konten sejarah yang lebih hidup dan mudah dipahami. Bahkan dalam ranah kesehatan, peneliti mulai mengeksplorasi *deepfake* sebagai sarana terapi, seperti membantu pasien dengan gangguan

bicara melalui sintesis suara yang lebih personal (Pasham, 2023). Dengan demikian, pada tahap awal, *deepfake* identik dengan optimisme terhadap kreativitas, inovasi, dan kemajuan teknologi.

Namun, perkembangan teknologi ini dengan cepat menimbulkan sisi gelap yang tidak bisa diabaikan. Seiring kemampuan teknis *deepfake* yang semakin mudah diakses publik melalui aplikasi open-source, muncul pula potensi penyalahgunaan dalam skala besar. Konten pornografi non-konsensual dengan wajah figur publik, video politik palsu yang digunakan untuk menyebarkan disinformasi, hingga penipuan keuangan berbasis manipulasi suara, menjadi bukti nyata bagaimana *deepfake* telah bertransformasi dari inovasi menjadi ancaman (Chesney & Citron, 2019). Bahkan lembaga keamanan internasional, seperti Europol dan FBI telah mengeluarkan peringatan tentang bahaya *deepfake* terhadap keamanan siber, stabilitas politik, dan kepercayaan publik terhadap institusi demokrasi.

Di Indonesia, wacana mengenai *deepfake* mulai mengemuka menjelang periode pemilu. Hal ini bukan tanpa alasan. Dengan tingkat penetrasi internet yang tinggi dan budaya konsumsi informasi digital yang masif, masyarakat Indonesia menjadi sasaran empuk bagi penyebaran hoaks dan manipulasi media (Surbakti, 2025). Kekhawatiran terhadap kemungkinan digunakannya teknologi *deepfake* untuk memanipulasi opini publik semakin besar, mengingat pengalaman sebelumnya di mana disinformasi berbasis media sosial mampu memengaruhi dinamika politik nasional. Diskursus ini tidak hanya muncul di kalangan akademisi, melainkan juga telah menjadi perhatian pemerintah, lembaga keamanan, serta organisasi masyarakat sipil yang menyoroti rendahnya literasi digital masyarakat Indonesia sebagai faktor kerentanan (Surbakti, 2024).

Fenomena global memperkuat urgensi isu ini. Pada tahun 2022, misalnya, dunia dikejutkan oleh video palsu Presiden Ukraina Volodymyr Zelensky yang menyerukan rakyatnya untuk menyerah dalam konflik dengan Rusia (Glick, 2023). Video tersebut sempat menyebar di berbagai platform media sosial sebelum akhirnya terbongkar sebagai *deepfake*. Kasus ini menunjukkan bahwa teknologi *deepfake* telah digunakan dalam konteks geopolitik dan peperangan informasi. Di sektor ekonomi, sebuah perusahaan energi di Inggris dilaporkan mengalami kerugian lebih dari €200.000 akibat panggilan telepon yang menggunakan suara *deepfake*

menyerupai CEO induk perusahaan (Stupp, 2019). Sementara itu, industri hiburan dan dunia selebritas menghadapi maraknya penyebaran konten pornografi palsu yang menggunakan wajah artis terkenal, seperti Scarlett Johansson dan Gal Gadot, yang menimbulkan kerugian reputasi dan trauma psikologis (Maddocks, 2020).

Dari contoh-contoh di atas terlihat jelas bahwa *deepfake* bukan lagi sekadar fenomena eksperimental atau isu teknis terbatas, melainkan ancaman nyata yang berdampak multidimensi. Tantangan terbesar yang muncul adalah bagaimana masyarakat dapat membedakan antara realitas dan rekayasa digital ketika batas antara keduanya semakin kabur (Vaccari & Chadwick, 2020). Hal ini membawa implikasi serius bagi demokrasi, karena kepercayaan publik terhadap informasi merupakan fondasi utama dalam proses pengambilan keputusan politik. Jika masyarakat tidak lagi mampu membedakan kebenaran, maka ruang publik akan dipenuhi dengan ketidakpastian dan keraguan, yang pada akhirnya melemahkan legitimasi demokrasi.

Selain itu, fenomena *deepfake* juga memunculkan persoalan etika dan hukum yang kompleks. Dari sisi etika, terdapat pelanggaran terhadap privasi dan martabat individu yang wajah atau suaranya digunakan tanpa izin (Kira, 2024). Dari sisi hukum, banyak yurisdiksi belum memiliki regulasi khusus yang secara eksplisit mengatur penggunaan dan distribusi *deepfake*. Di beberapa negara, hukum yang ada masih menggunakan pasal umum tentang penipuan, pencemaran nama baik, atau pelanggaran hak cipta untuk menangani kasus *deepfake*. Namun, pendekatan ini terbukti tidak cukup adaptif mengingat kompleksitas dan kecepatan perkembangan teknologi (Chawki, 2024).

Indonesia sendiri masih berada pada tahap awal dalam menanggapi fenomena ini. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dapat dijadikan payung hukum untuk menjerat pelaku, namun UU tersebut belum secara spesifik menyebutkan atau mengantisipasi teknologi *deepfake* (Putri et al., 2024). Sementara itu, literasi publik mengenai bahaya dan modus penyalahgunaan *deepfake* masih relatif rendah, sehingga memperbesar peluang manipulasi.

Melihat perkembangan tersebut, jelas bahwa kajian akademik tentang tipologi penyalahgunaan, contoh konkret, serta regulasi global terkait

deepfake menjadi sangat penting. Pertama, tipologi penyalahgunaan diperlukan untuk memahami secara sistematis bentuk-bentuk ancaman yang ditimbulkan. Kedua, contoh konkret dari berbagai kasus akan membantu memberikan gambaran nyata tentang kerugian yang diakibatkan oleh *deepfake*. Ketiga, telaah regulasi global dapat menjadi inspirasi dan referensi bagi Indonesia dalam menyusun kebijakan yang sesuai dengan konteks nasional.

Dengan demikian, bab ini berupaya menjawab kebutuhan tersebut dengan membahas fenomena *deepfake* secara komprehensif. Fokus utama diarahkan pada klasifikasi tipologi penyalahgunaan, analisis kasus nyata baik di tingkat global maupun Indonesia, serta kajian perbandingan regulasi internasional. Harapannya, pembahasan ini dapat memperkaya literatur akademik sekaligus memberikan masukan praktis bagi pembuat kebijakan, praktisi, dan masyarakat luas dalam menghadapi tantangan yang ditimbulkan oleh *deepfake*.

BAB
2

GAMBARAN UMUM, TREN, DAN RISIKO TEKNOLOGI *DEEPFAKE*

1. Pengantar Teknologi *Deepfake*

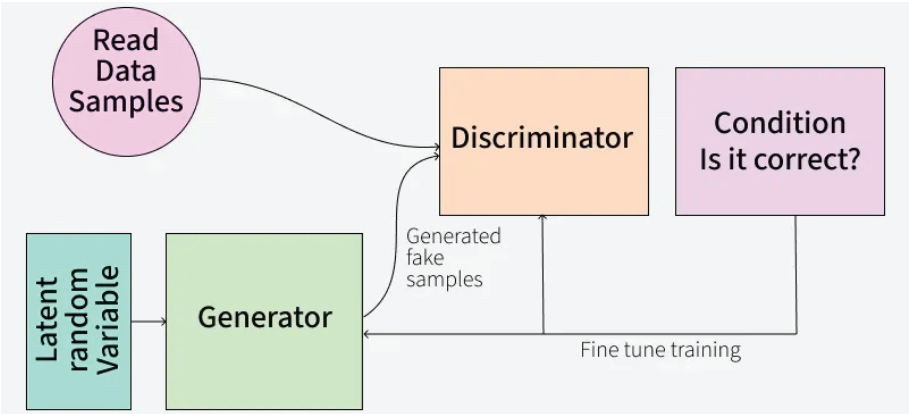
Teknologi *deepfake* merupakan sebuah teknologi yang memanfaatkan kecerdasan buatan atau Artificial Intelligence (AI) khususnya dalam bidang machine learning dan deep learning. Teknologi ini mampu memanipulasi bahkan membuat suatu konten visual dan audio secara hiperrealistis dalam menirukan atau mengganti identitas sesorang. Sehingga konten berupa video, gambar, ataupun suara yang dihasilkan dari teknologi *deepfake* ini susah dibedakan jika dibandingkan dengan konten yang asli (Noval, 2019).

Berbeda dengan rekayasa digital secara konvensional yang menggunakan berbagai alat bantu seperti aplikasi untuk edit video, suara, maupun video. Teknik ini dilakukan oleh manusia dan membutuhkan ketelitian dan kesabaran dalam pengeditan dikarenakan dibutuhkan waktu yang cukup lama untuk mengedit setiap detail gambar supaya terlihat realistis dan detail. Biasanya rekayasa digital secara konvensional ini masih memiliki kelemahan yaitu meninggalkan jejak manipulasi yang relatif mudah dikenali, seperti ketidakseimbangan pencahayaan, kualitas suara yang berbeda, atau penggunaan efek yang terlalu mencolok atau berlebihan.

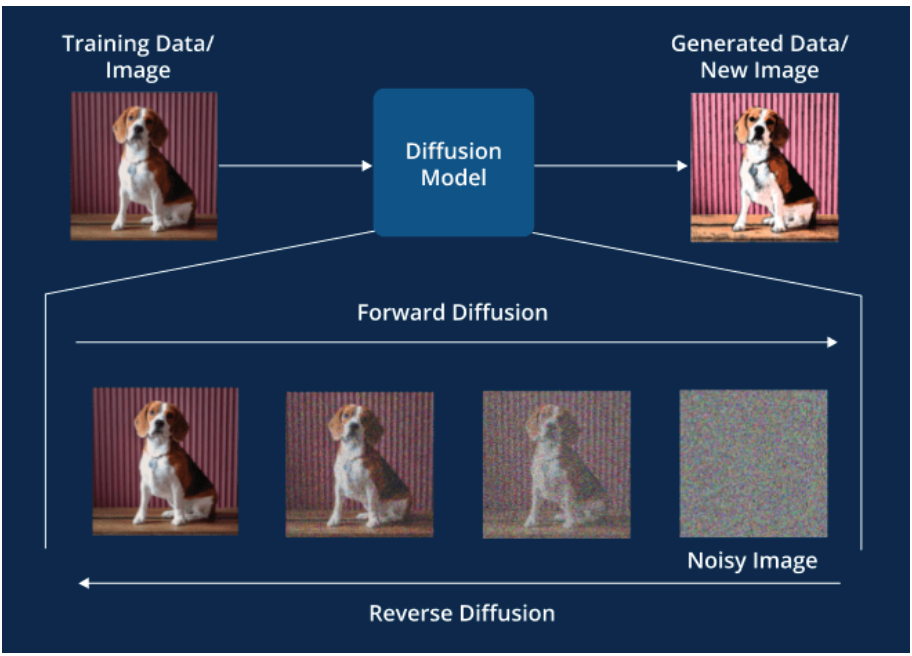
Sebaliknya dengan teknologi *deepfake* dapat mempelajari pola dan fitur wajah, suara, ataupun gerakan tubuh seseorang, lalu dapat

merekonstruksinya secara otomatis. Maka dengan membutuhkan waktu beberapa menit atau bahkan beberapa detik saja, teknologi ini dapat membuat konten yang hiperrealistis tanpa upaya yang banyak, hanya menggunakan perintah yang diinput (command prompt) ke dalam aplikasi tersebut, maka teknologi *deepfake* dapat membuat sesuatu konten sesuai perintah, bahkan konten yang jika dalam dunia nyata dikatakan mustahil terjadi dapat tetap dibuat dan hasilnya terlihat realistis.

Pada umumnya terdapat dua pendekatan utama yang sering digunakan dalam pembuatan *deepfake* yaitu Generative Adversarial Networks (GAN) dan diffusion model. GAN adalah salah satu cabang pendekatan dari jaringan saraf tiruan manusia, maka jika dilihat dari cara kerja GAN ini dapat menyerupai cara kerja otak manusia. Terdapat jaringan saraf generator yang bertugas untuk menghasilkan konten sintetis dan jaringan saraf discriminator yang bertugas membedakan apakah konten tersebut asli atau tidak. Kedua jaringan saraf tersebut saling berkompetisi secara berulang, sehingga konten yang dihasilkan oleh generator menjadi semakin realistis karena akan terus disempurnakan untuk menipu discriminator (Say, Alkan, & Kocak, 2025) seperti terlihat pada Gambar 1. Sedangkan Diffussion model adalah pendekatan yang lebih baru dibanding GAN. Model ini mampu bekerja dengan cara menambahkan noise atau istilah lainnya merusak pada data aslinya secara bertahap, lalu melatih AI untuk mengembalikan data tersebut menjadi bentuk yang utuh kembali (Chen, Haldar, Akhtar, & Mian, 2023) seperti terlihat pada Gambar 2. Dengan menggunakan proses pembelajaran tersebut, AI mampu menciptakan konten sintetis yang sangat detail, termasuk tekstur kulit, ekspresi wajah, intonasi suara, bahkan berbagai detail lainnya. Model ini dikenal sebagai teknologi di balik perkembangan pesat text-to-image atau text-to-video generation dalam beberapa tahun terakhir.



Gambar 1. Arsitektur *Generative Adversarial Networks* (GAN)
(Sumber: https://www.geeksforgeeks.org/deep-learning/generative-adversarial-network-gan/)



Gambar 2. Arsitektur *Diffusion Model*
(Sumber: https://www.leewayhertz.com/diffusion-models/)

Pemanfaatan kedua model tersebut menjadikan *deepfake* sebagai salah satu inovasi AI generatif yang sangat maju dan kontroversial, karena diakui dalam menciptakan konten yang nyaris mustahil untuk dibedakan dengan

kenyataan. Teknologi *deepfake* disini pastinya tidak terlepas hubungannya dengan data biometrik, dimana teknologi ini memanfaatkan data pribadi yang didasarkan pada karakteristik biologis dan perilaku individu (Maghrabi, 2025). Umumnya terdapat 3 bentuk utama biometrik yang sering digunakan untuk tindakan manipulasi yaitu wajah, suara, dan gerakan tubuh. Disini data wajah merupakan target utama dalam teknologi *deepfake*, dengan memanfaatkan berbagai kumpulan foto atau video seseorang sebagai data latih, maka algoritma *deepfake* mampu mempelajari pola ekspresi dan struktur wajah. Selain itu suara dan gerakan tubuh juga dipelajari untuk melihat berbagai jenis suara, intonasi, sinkronisasi antara gerakan bibir dengan suara, berbagai pola gerakan seperti duduk, berdiri, berjalan, dan berbagai aktivitas lainnya yang dilakukan manusia secara alami (Wu, 2025; Hosny & Mahfouz, 2025).

2. Tren Perkembangan dalam 5 Tahun ke Depan

Teknologi *deepfake* diprediksi akan berkembang secara eksponensial seiringan dengan berkembangannya infrastruktur utama yang dibutuhkan dalam teknologi ini seperti meningkatnya kemampuan komputasi, ketersediaan dataset biometrik, dan penyempurnaan algoritma generatif AI (A Comprehensive Guide to Generative Adversarial Networks (GANs) and Application to Individual Electricity Demand, 2024; Pei, et al., 2024). Data Sensity AI mencatat peningkatan sebanyak 550 persen konten *deepfake* dalam 5 tahun terakhir. Laporan tersebut juga ditanggapi oleh Kemkomdigi untuk mendorong para penyedia platform global menyediakan fitur cek konten AI seperti terlihat pada Gambar 3. Negara Indonesia yang saat ini masuk dalam salah satu jumlah pengguna internet terbesar di dunia, maka memliki potensi menjadi arena yang sangat rentan terhadap penggunaan dan penyebaran konten *deepfake*, baik dalam tujuan positif maupun negatif.

Gambar 3. Siaran Pers dari Website Komdigi Terkait Kenaikan Penggunaan *Deepfake* (Sumber: https://www.komdigi.go.id/berita/siaran-pers/detail/*deepfake*-naik-550-kemkomdigi-minta-platform-global-sediakan-fitur-cek-konten-ai)

Secara global, kita dapat melihat peningkatan pada akses perangkat lunak berbasis AI open-source dapat mempercepat produk konten *deepfake* tersebut. Selain itu model generatif AI yang semula membutuhkan perangkat keras khusus dengan spesifikasi yang canggih, kini dapat dijalankan pada komputer personal dengan kapasitas menengah ke bawah, bahkan bisa juga dijalankan dalam sebuah perangkat smartphone. Hal ini memperkecil hambatan masuk bagi individu atau kelompok dalam membuat konten sintetis berkualitas tinggi. Jika melihat pertumbuhan pengguna media sosial yang masif serta penetrasi smartphone yang hampir merata dalam berbagai kalangan usia, status, daerah, dan tersebar berbagai belahan dunia, maka hal ini memperbesar potensi distribusi konten *deepfake*. Maka jika tidak disertai regulasi dan literasi digital yang memadai, maka dalam 5 tahun ke depan dapat menghadapi lonjakan kasus penyalahgunaan *deepfake* yang sangat serius mulai dari ranah politik, ekonomi, maupun sosial budaya (Seveney, Wicaksono, & Soetijono, 2025).

Melihat beberapa perkembangan yang ada di saat ini dibanding beberapa tahun lalu, teknologi *deepfake* sekarang sudah mulai tersebar digunakan dalam berbagai bidang seperti industri film dan hiburan,

edukasi, iklan dan pemasaran, dan komunikasi visual. Seperti contohnya studio film yang menggunakan teknologi ini untuk merekonstruksi wajah tokoh sejarah atau aktor yang sudah meninggal atau untuk mengurangi biaya produksi efek visual (Lees, 2024; Okeke, Nwosu, Asogwa, & Dada, 2024). Penggunaan teknologi *deepfake* ini dapat memiliki nilai positif bagi manusia jika dimanfaatkan secara benar, namun seperti yang kita tahu bahwa setiap teknologi pasti memiliki celah atau dampak risiko jika digunakan secara sembarangan. Beberapa perkembangan pesat terkait risiko yang dapat kita lihat di sekitar kita adalah terkait politik seperti manipulasi pidato atau video tokoh publik untuk menyebarkan disinformasi yang dapat memicu konflik atau merusak reputasi, meningkatnya kriminalitas digital seperti pemalsuan suara pejabat atau eksekutif untuk menipu lembaga keuangan dan perusahaan (Nurdin & Nugraha, 2025), penipuan identitas dengan menggunakan wajah atau suara hasil rekayasa untuk membuka rekening bank, mengakses akun pribadi, atau bahkan melewati sistem autentikasi biometrik, serta meningkatnya kasus pornografi non-konsensual yang menjadi salah satu bentuk penyalahgunaan paling dominan, dimana wajah individu ditempelkan pada konten pornografi tanpa izin (Pitaloka, 2025).

Berdasarkan kajian, beberapa sektor yang diperkirakan akan mengalami dampak paling signifikan dalam beberapa tahun ke depan adalah keamanan dan pertahanan, keuangan, media sosial, dan industri hiburan (Widjaja, 2025). Potensi disinformasi masif melalui video manipulatif ini dapat melemahkan stabilitas politik dan keamanan nasional, kemudian lembaga perbankan dan fintech yang mengandalkan verifikasi biometrik juga berpotensi menjadi sasaran utama dalam serangan *deepfake*, selanjutnya platform digital yang berperan sebagai jalur distribusi utama konten *deepfake* rentan menjadi ekosistem penyebaran hoaks, selain itu dalam dunia hiburan dapat meningkatkan pelanggaran hak cipta dan eksploitasi aktor.

BAB
3

TIPOLOGI PENYALAHGUNAAN *DEEPFAKE*

Perkembangan teknologi *deepfake* telah melahirkan berbagai bentuk penyalahgunaan yang kompleks dan berimplikasi luas. Kategori penyalahgunaan ini penting dipahami agar pembuat kebijakan, peneliti, maupun masyarakat dapat mengidentifikasi pola ancaman sekaligus menyiapkan langkah mitigasi yang tepat. Berdasarkan kajian literatur akademik (Chesney & Citron, 2019; Vaccari & Chadwick, 2020), tipologi penyalahgunaan *deepfake* dapat diklasifikasikan ke dalam enam kategori utama: penyalahgunaan identitas; manipulasi informasi dan reputasi; kejahatan finansial dan siber; eksploitasi sosial dan psikologis; penyalahgunaan dalam domain hukum dan forensik; serta penyalahgunaan massal dan sistemik.

1. Penyalahgunaan Identitas

Penyalahgunaan identitas merupakan salah satu bentuk paling langsung dari teknologi *deepfake*. Modus ini dilakukan dengan memanfaatkan wajah, suara, atau ciri khas seseorang untuk kepentingan tertentu tanpa seizin pemilik identitas tersebut. Dalam konteks sosial, penyalahgunaan identitas biasanya menargetkan figur publik seperti selebriti, politisi, atau tokoh masyarakat karena pengaruh mereka yang luas (Kietzmann et al., 2020). Namun, kasus-kasus terbaru menunjukkan bahwa orang biasa juga bisa menjadi korban, misalnya melalui pemalsuan video konferensi kerja yang digunakan untuk menipu kolega atau atasan.

Contoh paling umum dari penyalahgunaan identitas adalah penggunaan wajah selebriti pada iklan atau konten daring tanpa izin. Kasus semacam ini bukan hanya melanggar hak atas privasi dan integritas personal, tetapi juga berpotensi menimbulkan kerugian finansial, karena citra tokoh publik merupakan aset ekonomi yang sering dikaitkan dengan kontrak komersial. Dari sisi hukum, kasus ini sulit ditangani karena batas antara parody, satire, dan penyalahgunaan yang merugikan masih kabur (Chesney & Citron, 2019).

Lebih jauh, penyalahgunaan identitas dengan teknologi *deepfake* juga menimbulkan persoalan serius dalam konteks keamanan pribadi. Misalnya, penggunaan suara seseorang yang dipalsukan dapat dimanfaatkan untuk mengakses layanan perbankan yang menggunakan sistem autentikasi berbasis voice recognition. Kasus serupa juga terjadi pada perusahaan yang menerapkan verifikasi suara dalam layanan pelanggan, di mana pelaku berhasil menipu sistem dengan menirukan suara pejabat tertentu melalui *deepfake* audio. Hal ini memperlihatkan bahwa penyalahgunaan identitas tidak hanya menyasar ranah publik, tetapi juga berpotensi mengancam aspek privasi dan keamanan finansial individu.

Selain itu, ancaman penyalahgunaan identitas diperkuat oleh kemudahan akses teknologi *deepfake* di ruang digital. Saat ini, berbagai aplikasi berbasis AI memungkinkan pengguna awam membuat video manipulatif hanya dengan mengunggah foto atau rekaman singkat. Demokratisasi teknologi ini memang memiliki nilai positif dalam kreativitas digital, namun sekaligus memperbesar risiko eksploitasi identitas tanpa batasan yang jelas (Mirsky & Lee, 2021). Kondisi ini menimbulkan dilema etis sekaligus menegaskan urgensi regulasi yang dapat menyeimbangkan inovasi dengan perlindungan hak individu.

Di Indonesia, kasus penyalahgunaan identitas melalui *deepfake* mulai menarik perhatian publik terutama dalam bentuk video atau foto manipulatif yang melibatkan artis dan tokoh politik. Misalnya, sejumlah selebriti perempuan Indonesia menjadi korban penyebaran video pornografi palsu dengan wajah mereka yang diganti melalui teknologi *deepfake*. Meskipun cepat dibantah oleh korban dan tim hukum mereka, kasus semacam ini menimbulkan kerugian reputasi yang sulit dipulihkan serta memicu trauma psikologis. Pada ranah politik, menjelang Pemilu 2024 sempat beredar

kekhawatiran bahwa *deepfake* dapat digunakan untuk menyebarkan ujaran atau pernyataan palsu seolah-olah berasal dari kandidat tertentu. Walaupun hingga kini belum ada kasus besar yang terverifikasi, potensi ini tetap menjadi ancaman serius terhadap kualitas demokrasi di Indonesia.

Konteks Indonesia menunjukkan bahwa penyalahgunaan identitas melalui *deepfake* tidak hanya menimpa figur internasional, melainkan juga sudah nyata dialami oleh masyarakat lokal. Kerentanan ini semakin diperparah dengan rendahnya literasi digital sebagian masyarakat, yang membuat mereka mudah percaya pada konten visual meskipun tidak terverifikasi. Oleh karena itu, penyalahgunaan identitas berbasis *deepfake* di Indonesia perlu mendapat perhatian khusus, baik melalui pendekatan hukum maupun edukasi publik, agar tidak berkembang menjadi ancaman sosial yang lebih luas.

2. Manipulasi Informasi dan Reputasi

Kategori kedua adalah manipulasi informasi dan reputasi, di mana *deepfake* digunakan untuk menyebarkan disinformasi atau merusak citra seseorang. Penyalahgunaan ini kerap muncul dalam konteks politik, khususnya menjelang pemilu, ketika opini publik sangat mudah dipengaruhi oleh berita visual (Vaccari & Chadwick, 2020). Video politik *deepfake* dapat menampilkan seorang kandidat yang seolah-olah menyampaikan pernyataan kontroversial, padahal sebenarnya tidak pernah diucapkan. Ancaman ini berimplikasi langsung terhadap demokrasi digital. Kepercayaan publik terhadap media visual, yang selama ini dianggap sebagai bukti paling autentik, terkikis ketika konten palsu semakin sulit dibedakan dari konten asli. Dalam konteks global, kasus video palsu Presiden Ukraina Volodymyr Zelensky pada 2022 menjadi ilustrasi nyata bagaimana *deepfake* digunakan untuk tujuan manipulasi geopolitik. Jika tren ini terus berlanjut tanpa regulasi yang efektif, maka demokrasi berpotensi terjebak dalam "era pasca-kebenaran" di mana fakta dan fiksi bercampur tanpa batas yang jelas.

Di Indonesia, manipulasi informasi melalui *deepfake* mulai mendapat perhatian serius, khususnya dalam kontestasi politik. Misalnya, menjelang Pemilu 2024, beredar konten audio dan video yang diduga menggunakan teknologi mirip *deepfake* untuk membuat suara tokoh politik terdengar seolah-olah menyampaikan pernyataan yang memicu perpecahan.

Walaupun sebagian besar dapat dibantah dan terbukti palsu, penyebaran yang sangat cepat di media sosial membuat dampaknya tidak bisa diabaikan. Publik sempat terpecah antara yang mempercayai keaslian konten dan yang meragukannya, sehingga reputasi kandidat tertentu ikut terpengaruh. Fenomena ini menunjukkan betapa rapuhnya ekosistem informasi digital di Indonesia terhadap serangan berbasis manipulasi teknologi.

Selain itu, kasus manipulasi reputasi juga terjadi di luar konteks politik, misalnya dalam dunia bisnis dan hiburan. Sejumlah figur publik di Indonesia, termasuk artis dan influencer, pernah menjadi korban video atau gambar yang dimanipulasi sehingga menampilkan mereka dalam situasi yang merugikan, seperti terlibat dalam skandal yang tidak pernah terjadi. Kasus-kasus seperti ini bukan hanya merusak nama baik, tetapi juga berpotensi mengganggu kontrak kerja sama komersial, merusak citra personal, hingga berdampak pada kesehatan mental korban. Hal ini memperlihatkan bahwa ancaman *deepfake* dalam manipulasi informasi dan reputasi di Indonesia tidak terbatas pada lingkup politik saja, tetapi juga merambah ke sektor sosial dan ekonomi.

3. Kejahatan Finansial dan Siber

Selain politik, dunia keuangan juga rentan terhadap penyalahgunaan *deepfake*. Modus CEO fraud menggunakan suara sintetis merupakan salah satu bentuk serangan yang paling banyak dilaporkan. Pada 2019, seorang CEO perusahaan energi di Inggris ditipu lebih dari €200.000 setelah menerima panggilan telepon dengan suara *deepfake* yang menyerupai atasan perusahaan induknya (Stupp, 2019). Kasus ini menunjukkan bahwa *deepfake* bukan hanya ancaman reputasi, melainkan juga dapat dimanfaatkan untuk penipuan finansial berskala besar.

Bentuk lain adalah phishing 2.0, di mana pelaku tidak hanya mengirimkan email palsu, tetapi juga memalsukan video atau suara yang meyakinkan korban untuk memberikan informasi sensitif. Dengan demikian, keamanan siber tradisional yang sebelumnya hanya berfokus pada teks dan tautan kini harus menghadapi tantangan baru berupa konten multimedia yang sangat realistis. Situasi ini menuntut perusahaan mengembangkan sistem verifikasi identitas yang lebih kuat, termasuk penggunaan autentikasi biometrik dan kode verifikasi multi-lapis.

Di Indonesia, modus penipuan berbasis *deepfake* juga mulai bermunculan, terutama dalam bentuk social engineering yang dikombinasikan dengan manipulasi suara. Pada 2023, sempat ramai kasus penipuan dengan modus panggilan video WhatsApp yang menggunakan wajah tiruan seorang pejabat bank untuk meyakinkan korban agar mentransfer sejumlah uang. Walaupun jumlah kerugian yang tercatat tidak sebesar kasus di Eropa atau Amerika, pola ini memperlihatkan eskalasi teknik penipuan di Indonesia dari sekadar phishing berbasis teks menjadi serangan berbasis audio-visual yang lebih meyakinkan. Hal ini memunculkan urgensi bagi perbankan nasional dan OJK untuk meningkatkan literasi keamanan digital di kalangan nasabah.

Selain itu, terdapat pula fenomena investasi bodong dan pinjaman online ilegal yang memanfaatkan teknologi manipulasi video untuk menampilkan testimoni palsu seolah-olah berasal dari tokoh publik atau influencer terkenal di Indonesia. Beberapa konten *deepfake* diunggah di media sosial dengan menampilkan figur populer, misalnya artis atau pejabat, yang "mengajak" masyarakat berinvestasi atau menggunakan aplikasi tertentu. Praktik ini tidak hanya merugikan korban secara finansial, tetapi juga menciptakan ketidakpercayaan publik terhadap figur publik yang sebenarnya tidak pernah terlibat. Hal ini menandakan bahwa kejahatan finansial berbasis *deepfake* di Indonesia semakin variatif, melibatkan aktor lintas sektor, dan menuntut respons regulasi yang lebih ketat.

4. Eksploitasi Sosial dan Psikologis

Eksploitasi sosial dan psikologis adalah kategori penyalahgunaan yang paling banyak mendapat sorotan publik, terutama terkait pornografi non-konsensual. Menurut laporan Kshetri (2023), sekitar 96% dari semua konten *deepfake* yang beredar di internet adalah pornografi, sebagian besar menampilkan wajah perempuan tanpa persetujuan mereka. Hal ini menimbulkan dampak serius berupa kerusakan reputasi, pelecehan daring, hingga trauma psikologis yang mendalam bagi korban.

Kasus-kasus pornografi *deepfake* sering melibatkan selebriti, tetapi tidak jarang pula perempuan biasa menjadi target, misalnya dalam kasus cyberbullying atau balas dendam personal. Karakteristik anonim internet memperparah situasi, karena pelaku sering kali sulit dilacak, sementara korban menghadapi beban ganda berupa stigma sosial dan kesulitan hukum.

Situasi ini menyoroti pentingnya kerangka hukum yang tegas serta upaya peningkatan literasi digital untuk melindungi kelompok rentan, terutama perempuan dan anak.

Di Indonesia, fenomena *deepfake* pornografi non-konsensual sudah mulai terdeteksi dalam beberapa tahun terakhir. Salah satu kasus yang mendapat perhatian publik adalah penyebaran video palsu yang menampilkan wajah artis tanah air pada tubuh orang lain dalam konten pornografi. Meskipun cepat dibantah dan diklarifikasi oleh pihak artis, kerusakan reputasi dan dampak psikologis tetap tidak terhindarkan. Kasus serupa juga dialami oleh sejumlah mahasiswi dan pekerja kantoran, di mana wajah mereka disalahgunakan oleh pelaku untuk membuat konten palsu sebagai bentuk balas dendam pribadi. Hal ini membuktikan bahwa korban bukan hanya figur publik, tetapi juga masyarakat biasa yang rentan menjadi sasaran eksploitasi digital.

Selain itu, kasus penipuan relasi daring (online dating scam) di Indonesia mulai memanfaatkan teknologi *deepfake* untuk menciptakan identitas palsu. Pelaku menggunakan foto atau video *deepfake* untuk meyakinkan korban bahwa mereka sedang berinteraksi dengan orang yang nyata. Setelah korban terikat secara emosional, pelaku kemudian memanfaatkan hubungan tersebut untuk meminta uang, hadiah, atau data pribadi. Praktik ini memperlihatkan bagaimana *deepfake* tidak hanya berdampak pada reputasi, tetapi juga dapat mengikis rasa percaya dalam interaksi sosial digital, menciptakan trauma emosional yang berkepanjangan bagi korban.

5. Penyalahgunaan dalam Domain Hukum dan Forensik

Tipologi berikutnya adalah penyalahgunaan *deepfake* dalam domain hukum dan forensik. Konten *deepfake* berpotensi digunakan sebagai bukti palsu dalam persidangan atau investigasi kriminal. Hal ini menjadi tantangan besar bagi aparat penegak hukum karena kemampuan manusia maupun sistem forensik tradisional untuk membedakan konten asli dan palsu semakin terbatas (Mirsky & Lee, 2021).

Misalnya, rekaman suara *deepfake* dapat digunakan untuk menuduh seseorang melakukan kejahatan, sementara video palsu bisa dipakai sebagai "barang bukti" untuk memperkuat narasi tertentu. Konsekuensinya sangat serius: tidak hanya berpotensi menjebak orang tak bersalah, tetapi juga

melemahkan kepercayaan masyarakat terhadap sistem peradilan. Jika bukti digital tidak lagi dapat diandalkan, maka prinsip rule of law bisa terganggu. Oleh karena itu, lembaga forensik digital saat ini gencar mengembangkan teknologi deteksi berbasis blockchain dan digital watermarking untuk menjamin keaslian bukti.

Di Indonesia, potensi penyalahgunaan *deepfake* dalam ranah hukum mulai terlihat dalam kasus-kasus rekayasa bukti digital. Misalnya, terdapat laporan mengenai penggunaan rekaman suara yang dipalsukan untuk memperkuat tuduhan dalam sengketa bisnis dan kasus kriminal. Walaupun sebagian besar masih dapat dibantah melalui analisis ahli, kasus ini menunjukkan celah berbahaya ketika bukti audio-visual dapat dimanipulasi sedemikian rupa sehingga tampak autentik. Situasi ini semakin krusial karena sistem peradilan Indonesia dalam beberapa tahun terakhir mulai membuka diri pada penggunaan bukti digital, sehingga validitas konten multimedia menjadi isu utama yang tidak bisa diabaikan.

Selain itu, potensi *deepfake* juga muncul dalam konteks propaganda dan framing oleh kelompok tertentu yang mencoba memengaruhi opini publik terkait kasus hukum. Misalnya, beredarnya video yang dimanipulasi untuk menggiring persepsi bahwa seorang pejabat atau aparat penegak hukum terlibat dalam praktik korupsi atau kekerasan, padahal video tersebut bukan bukti yang sah. Jika dibiarkan, praktik semacam ini tidak hanya merusak reputasi individu, tetapi juga mengikis legitimasi lembaga hukum di mata masyarakat. Dengan demikian, tantangan bagi Indonesia bukan hanya mendeteksi *deepfake*, tetapi juga memastikan ada payung hukum yang jelas mengenai penerimaan atau penolakan bukti digital dalam persidangan.

6. Penyalahgunaan Massal dan Sistemik

Kategori terakhir adalah penyalahgunaan massal dan sistemik, yaitu penggunaan *deepfake* sebagai bagian dari strategi operasi informasi oleh negara atau aktor non-negara. Kasus yang sering disebut adalah dugaan penggunaan synthetic media oleh Rusia dan Tiongkok dalam operasi geopolitik untuk memengaruhi opini publik internasional.

Dalam skala besar, penyalahgunaan ini dapat menciptakan ketidakstabilan sosial, memperburuk polarisasi politik, dan melemahkan kohesi masyarakat. Lebih jauh, *deepfake* juga dapat dimanfaatkan

dalam perang psikologis, misalnya dengan menyebarkan video palsu yang menurunkan moral militer atau menimbulkan kepanikan warga sipil. Konteks ini menunjukkan bahwa *deepfake* bukan hanya ancaman individual, melainkan juga ancaman sistemik terhadap keamanan nasional dan internasional.

Di Indonesia, potensi penyalahgunaan *deepfake* secara massal terlihat dari maraknya kampanye disinformasi menjelang Pemilu. Beberapa pengamat politik mencatat beredarnya video manipulatif di media sosial yang menampilkan tokoh politik tertentu seolah-olah memberikan pernyataan kontroversial terkait isu agama atau etnis. Walaupun tidak selalu terkonfirmasi sebagai *deepfake*, pola distribusi yang terkoordinasi memperlihatkan bagaimana teknologi ini dapat dipakai untuk memicu polarisasi sosial dalam skala luas. Jika dibiarkan, praktik semacam ini berpotensi memperlemah integritas pemilu serta menurunkan kepercayaan masyarakat terhadap institusi demokrasi.

Contoh nyata dari manipulasi informasi dan reputasi di Indonesia adalah kasus *deepfake* Menteri Keuangan Sri Mulyani yang dibuat seolah-olah menyatakan bahwa guru merupakan beban negara. Padahal, pernyataan tersebut tidak pernah diucapkan olehnya. Video palsu ini dengan cepat menyebar di media sosial dan memicu reaksi keras dari masyarakat. Dampaknya tidak hanya merusak citra pribadi Sri Mulyani sebagai pejabat publik, tetapi juga berujung kekerasan dalam bentuk penjarahan rumah beliau dan juga berhentinya karir Sri Mulyani sebagai Menteri Keuangan yang sudah dia jalani selama lebih dari 10 tahun.

Selain ranah politik, potensi penyalahgunaan sistemik *deepfake* juga muncul dalam konteks bencana dan keamanan nasional. Misalnya, terdapat kekhawatiran bahwa video *deepfake* dapat digunakan untuk menyebarkan kabar palsu mengenai kondisi pasca-bencana, seperti banjir atau gempa bumi, sehingga menimbulkan kepanikan massal atau menghambat proses evakuasi. Dalam situasi darurat, publik cenderung percaya pada informasi visual tanpa sempat melakukan verifikasi, sehingga aktor jahat dapat mengeksploitasi kondisi tersebut untuk memperburuk krisis. Hal ini menegaskan bahwa di Indonesia, *deepfake* tidak hanya menjadi masalah individu atau kelompok kecil, tetapi juga berpotensi mengancam stabilitas sosial dan keamanan negara secara menyeluruh.

BAB
4

ASESMEN RISIKO KEAMANAN, DAMPAK MERUGIKAN, DAN ANCAMAN TERHADAP DATA BIOMETRIK

Teknologi *deepfake* dapat membawa implikasi risiko yang sedemikian luasnya, mulai dari tingkat individu, organisasi, masyarakat, negara, hingga global. Kompleksitas ancaman *deepfake* bukan hanya sekedar di isu teknologi saja, namun menjadi tantangan multidimensi yang bersinggungan dengan data biometrik seseorang, hak privasi, keamanan, hingga ke arah nasional (Kusnadi & Putri, 2025).

1. Risiko terhadap Individu

Pada tingkat individu terdapat beberapa risiko seperti pencurian identitas dimana wajah atau suara hasil rekayasa diguanakan untuk mengakses layanan berbasis autentikasi biometrik, seperti perbankan atau aplikasi mobile lainnya; pemerasan dan pornografi non-konsensual dimana video palsu menggunakan wajah seseorang dan dimasukkan ke dalam sebuah konten video pornografi yang kerapnya diproduksi untuk tujuan menjatuhkan reputasi individu atau memeras korban; serta perundungan siber dimana penyebaran konten *deepfake* yang bertujuan mempermalukan individu. Beberapa risiko tersebut dapat memberikan dampak serius pada individu khususnya kesehatan mental, psikologi, finansial, hingga dapat menyebabkan kematian karena bunuh diri.

2. Risiko terhadap Organisasi

Pada tingkat organisasi terdapat beberapa risiko seperti fraud dan manipulasi internal seperti pemalsuan instruksi pimpinan sehingga merugikan organisasi; kerentanan sistem keamanan pada perusahaan khususnya yang menggunakan autentikasi biometrik dalam berbagai ruang lingkup pekerjaan seperti akses ruang kerja atau akses data sensitif; serta reputasi korporasi juga menjadi dampak risiko yang dapat merusak citra perusahaan, mempengaruhi harga saham, dan menurunkan kepercayaan publik terhadap perusahaan tersebut.

3. Risiko terhadap Masyarakat

Pada tingkat masyarakat terdapat beberapa risiko seperti disinformasi terhadap konten video manipulatif atau hoaks yang memperkuat penyebaran berita bohong dan sulit untuk diverifikasi; krisis kepercayaan publik dikarenakan munculnya fenomena liar's dividend ketika masyarakat mulai kehilangan kepercayaan terhadap bukti-bukti visual atau audio; serta disrupsi demokrasi dimana contohnya dalam proses pemilu yang terganggu jika opini publik dimanipulasi melalui *deepfake*. Risiko pada tingkatan ini sangat serius karena dapat meningkat hingga ke tingkat negara atau global, dimana salah satu contohnya krisis kepercayaan pada negara akibat dampak penggunaan *deepfake* tersebut.

4. Risiko terhadap Negara

Pada tingkat negara terdapat beberapa risiko seperti sabotase reputasi pejabat publik dengan memanipulasi atau membuat konten palsu untuk merusak legitimasi pemimpin; ancaman keamanan di tingkat nasional dikarenakan teknologi *deepfake* yang dapat dijadikan salah satu instrumen perang informasi oleh aktor asing; eksploiitasi infrastruktur vital seperti sistem keuangan atau energi berbasis autentikasi biometrik.

5. Risiko secara Global

Pada tingkat global terdapat beberapa risiko seperti memicu konflik internasional dengan menggunakan video palsu yang dapat memprovokatif tokoh atau pejabat di suatu negara; manipulasi pasar global seperti contohnya video atau audio palsu dari toko ekonomi dunia yang dapat memicu volatilitas pasar saham dan mata uang; cybercrime transnasional seperti pemanfaatan *deepfake* untuk menipu perusahaan multinasional atau mencuci uang melalui sistem keuangan global.

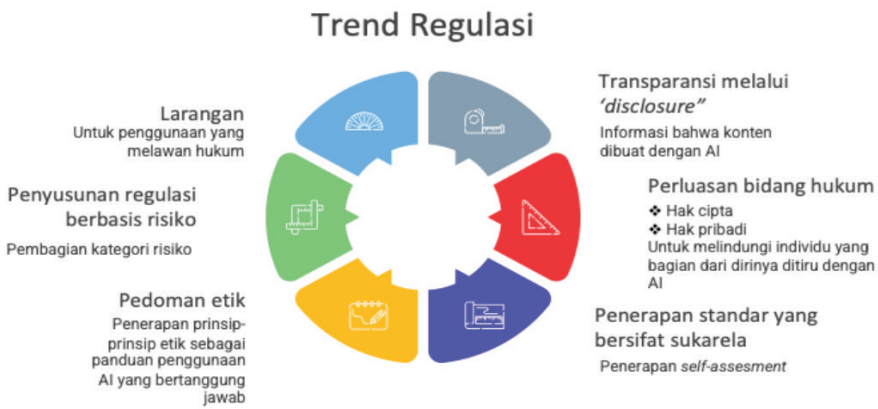
Melihat berbagai risiko tersebut, data biometrik menjadi salah satu hal yang paling penting karena data biometrik memiliki karakter permanen seperti wajah, suara, iris, dan sidik jari yang tidak dapat digantikan jika terjadi kebocoran data (Zahra, Hapsari, & Safitri, 2024). Teknologi *deepfake* ini mampu menembus sistem keamanan dengan menggunakan data biometrik seperti sistem autentikasi berbasis pengenalan wajah atau verifikasi suara.

BAB
5

TREN REGULASI: *BENCHMARKING* REGULASI TENTANG *DEEPFAKE* DI YURISDIKSI LAIN

Perkembangan teknologi *deepfake* telah menimbulkan tantangan serius di berbagai belahan dunia. Sifatnya yang mampu merekayasa suara, wajah, hingga video dengan kualitas realistis membuat *deepfake* mudah disalahgunakan untuk manipulasi informasi, penipuan finansial, hingga pelecehan seksual digital. Negara-negara merespons fenomena ini dengan pendekatan hukum yang berbeda-beda, mulai dari penekanan pada hak individu, regulasi transparansi, kriminalisasi konten intim, hingga kewajiban platform digital.

Dari sejumlah model regulasi yang digunakan di yurisdiksi yang dipelajari dalam studi ini, dapat diringkas tren regulasi sebagai berikut:



Gambar 4. Trend Regulasi.

Secara spesifik, bagian berikut menjelaskan regulasi *deepfake* di beberapa yurisdiksi utama.

1. Denmark

Denmark menjadi salah satu negara pelopor di Eropa dalam membentuk kerangka hukum khusus terkait *deepfake*. Pemerintah mengusulkan undang-undang yang memberikan hak kepemilikan hukum atas wajah dan suara kepada individu. Dengan demikian, setiap penggunaan *deepfake* yang menyerupai seseorang tanpa izin dapat dianggap melanggar hukum.

Undang-undang ini tidak hanya menyasar pelaku, tetapi juga platform digital. Jika platform gagal menghapus konten *deepfake* yang tidak sah, mereka dapat dikenai denda berat. Hal ini menandai pergeseran tanggung jawab ke perusahaan teknologi agar lebih proaktif dalam moderasi konten. Namun, Denmark juga menekankan adanya pengecualian untuk parodi dan satire, guna menjaga kebebasan berekspresi dan kreativitas seni. Meski demikian, batas antara ekspresi sah dan penyalahgunaan masih menjadi bahan diskusi publik.

Rancangan ini mendapat dukungan luas lintas partai di parlemen, dengan target implementasi akhir 2025 atau awal 2026. Jika berhasil, aturan Denmark dapat menjadi preseden global dalam perlindungan hak digital dan etika AI.

2. Amerika Serikat

Saat ini, belum ada undang-undang atau peraturan federal yang komprehensif di AS yang mengatur pengembangan AI, atau secara khusus melarang atau membatasi penggunaannya, termasuk *deepfake*. Namun, sejumlah negara bagian seperti California, Texas, dan Virginia sudah mengambil langkah. Mereka mengkriminalkan *deepfake* untuk tujuan politik (mis informasi pemilu) serta konten pornografi tanpa persetujuan. Di level federal, wacana *"AI Labeling Act"* muncul untuk mendorong penandaan konten sintetis secara eksplisit. Meskipun belum disahkan, dorongan ini mencerminkan kesadaran akan perlunya standar nasional.

Tantangan utama di AS adalah benturan dengan Amandemen Pertama (kebebasan berekspresi). Beberapa aturan, misalnya larangan distribusi *deepfake* politik menjelang pemilu, sempat mendapat perlawanan di

pengadilan dengan alasan berpotensi membatasi kebebasan berbicara. Kondisi ini membuat regulasi *deepfake* di AS cenderung fragmentaris dan inkonsisten antar negara bagian. Namun, kasus viral seperti *deepfake* Presiden Obama tahun 2018 untuk edukasi publik dan *deepfake* pornografi selebriti semakin meningkatkan urgensi regulasi.

Beberapa perkembangan terbaru terkait regulasi AI di Amerika Serikat dapat digambarkan sebagai berikut:

Pada tanggal 23 Januari 2025, Presiden Trump menandatangani Perintah Eksekutif baru berjudul ‚*Removing Barriers to American Leadership in Artificial Intelligence*' yang berfokus pada pencabutan kebijakan yang dianggap membatasi inovasi AI. Aspek utama di dalam Perintah Eksekutif ini antara lain adalah mengidentifikasi tindakan apa pun yang bertentangan dengan kebijakan baru dan bekerja sama dengan lembaga terkait untuk menangguhkan, merevisi, atau membatalkannya jika diperlukan. Selain itu, diberlakukannya *the National Artificial Intelligence Initiative* (NAII) tahun 2020 sebagai salah satu upaya nasional besar pertama yang secara khusus menargetkan kecerdasan buatan, dengan fokus utama lebih sedikit pada regulasi AI dan lebih pada pengembangan penelitian dan pengembangan di bidang tersebut dan bertujuan untuk memperkuat posisi Amerika Serikat sebagai pemimpin global dalam inovasi AI.

Dalam tingkat negara bagian, telah diadopsi sejumlah regulasi yang mengatur penggunaan AI, antara lain berikut ini:

a. Undang-Undang AI Colorado, berlaku sejak 17 Mei 2024, merupakan Undang-undang AI komprehensif pertama di AS. Undang-undang ini mengadopsi pendekatan berbasis risiko terhadap AI, mirip dengan Undang-Undang Uni Eropa, dan terutama menargetkan pengembang dan pengguna sistem AI berisiko tinggi.

b. Serangkaian Undang-Undang AI California, sejak September 2024, menggunakan pendekatan legislasi yang lebih terfragmentasi. Beberapa menetapkan aturan khusus untuk teknologi *deepfake*, yang lain untuk memastikan transparansi dalam AI, melindungi privasi data, atau menguraikan bagaimana AI dapat digunakan dalam layanan kesehatan. Sebagai contoh, Tennessee memberlakukan *Ensuring Likeness, Voice, and Image Security Act („ELVIS Act")* yang Maret 2024.

Mirip dengan legislasi di Denmark, undang-undang ini memperluas hak cipta dengan melarang penggunaan AI tanpa izin untuk meniru nama, foto, suara, atau rupa seseorang, tanpa lisensi. Berikutnya adalah *the Senate Bill 942 - California AI Transparency Act* - berlaku efektif 1 Januari 2026, dengan *‚Covered Providers‘* sistem AI yang dapat diakses publik di California dengan lebih dari satu juta pengunjung atau pengguna bulanan berkewajiban menerapkan langkah-langkah komprehensif untuk mengungkapkan ketika konten telah dihasilkan atau dimodifikasi oleh AI, menguraikan persyaratan untuk alat deteksi AI dan pengungkapan konten, dan menetapkan praktik perizinan untuk memastikan bahwa hanya sistem AI yang patuh yang diizinkan untuk penggunaan publik.

c. *Utah Artificial Intelligence Policy Act*, berlaku sejak Mei 2024: mewajibkan individu dan entitas untuk mengungkapkan penggunaan GenAI dalam komunikasi dengan konsumen.

d. *Texas Responsible AI Governance Act („TRAIGA“)*, berlaku sejak 22 Juni 2025, yang mencerminkan Undang-Undang AI Colorado dan Uni Eropa, secara signifikan mempersempit cakupannya dengan menghilangkan banyak kewajiban sektor swasta, tetapi tetap mempertahankan batasan kategoris pada pengembangan dan penerapan sistem AI untuk tujuan tertentu seperti manipulasi perilaku, diskriminasi yang melanggar hukum, dan pelanggaran hak konstitusional. Selain itu, sistem AI tidak boleh dikembangkan atau didistribusikan dengan tujuan tunggal untuk memproduksi, membantu, atau membantu dalam memproduksi, atau mendistribusikan video atau gambar *deepfake* yang melanggar hukum.

3. China

Sejak 2022, China menerapkan aturan “deep synthesis” yang mewajibkan semua konten *deepfake* untuk diberi label jelas sebagai buatan AI. Aturan ini menargetkan platform agar bertanggung jawab atas penyebaran konten. Selain itu, *deepfake* dilarang digunakan untuk menipu atau mencemarkan nama baik. Jika melanggar, platform wajib menghapus konten dengan segera, atau berhadapan dengan sanksi pemerintah.

Pendekatan China menekankan pengendalian *top-down*, selaras dengan strategi negara dalam mengelola ruang digital dan mencegah

penyebaran informasi yang dianggap berbahaya. Regulasi ini dianggap sebagai salah satu yang paling ketat di dunia, mencerminkan komitmen pemerintah untuk menekan risiko sosial, sekaligus mempertahankan stabilitas politik domestik.

4. India

India hingga kini belum memiliki undang-undang khusus *deepfake*. Namun, penyalahgunaan *deepfake* dapat dijerat dengan *IT Act* (untuk kejahatan siber) dan *Indian Penal Code* (IPC), misalnya pasal pencemaran nama baik. Seiring meningkatnya kasus pornografi *deepfake* dan penipuan daring, pemerintah India mulai mempertimbangkan kerangka regulasi baru untuk AI. Beberapa pejabat menyerukan perlunya undang-undang komprehensif yang menangani *deepfake* secara spesifik.

Selain jalur hukum, penanganan kasus sering dilakukan melalui kerja sama dengan platform media sosial untuk menurunkan konten yang melanggar. Namun, mekanisme ini masih bersifat ad hoc dan bergantung pada laporan publik. Tantangan di India adalah skala pengguna internet yang sangat besar, ditambah literasi digital masyarakat yang beragam. Hal ini membuat urgensi regulasi semakin tinggi agar perlindungan terhadap individu bisa lebih kuat.

5. Uni Eropa

Uni Eropa telah mengesahkan EU AI Act (2024) yang mengatur penggunaan AI, termasuk *deepfake*. Aturan ini mewajibkan konten *deepfake* ditandai secara eksplisit untuk melindungi publik dari disinformasi. Pelanggaran terhadap kewajiban ini dapat dikenai denda besar, hingga €35 juta atau 7% dari omzet global perusahaan. Sanksi ini menegaskan keseriusan Eropa dalam menegakkan regulasi.

Pendekatan UE berfokus pada prinsip *"transparency by design"*, termasuk metadata, waktu pembuatan, dan metode penandaan digital lainnya. Transparansi menjadi kunci dalam membangun kepercayaan publik. Selain itu, EU AI Act memberi landasan hukum bagi negara-negara anggota untuk mengembangkan kebijakan lebih rinci, sehingga menciptakan standar regional yang seragam dalam menangani ancaman *deepfake*.

6. Britania Raya

Inggris mengatur *deepfake* melalui *Online Safety Act 2023* yang diperkuat dengan amandemen pada 2024–2025. Regulasi ini secara khusus mengkriminalkan pembuatan dan distribusi konten intim non-konsensual berbasis *deepfake*. Hal ini lahir sebagai respons terhadap maraknya kasus pelecehan digital terhadap perempuan di media sosial. Pemerintah Inggris juga memperkuat kewenangan regulator Ofcom untuk mengawasi kepatuhan platform digital. Jika platform gagal menurunkan konten *deepfake* yang melanggar, mereka dapat dikenai sanksi berat, termasuk denda yang signifikan.

Selain aspek kriminalisasi, regulasi Inggris juga mengakui adanya pengecualian terbatas seperti parodi dan satire. Namun, perdebatan publik masih berlangsung tentang batasan antara kebebasan berekspresi dan perlindungan individu. Dengan kombinasi hukum pidana dan regulasi platform, Inggris berupaya menciptakan ekosistem online yang lebih aman, khususnya untuk mencegah eksploitasi seksual berbasis teknologi.

7. Korea Selatan

Korea Selatan termasuk negara yang sangat progresif dalam menindak kejahatan seksual digital. Pada 2024, pemerintah mengusulkan amandemen hukum yang mengkriminalkan tidak hanya produksi dan distribusi, tetapi juga kepemilikan dan konsumsi *deepfake* seksual. Langkah ini dilatarbelakangi oleh tingginya kasus pelecehan seksual berbasis gambar *(image-based abuse)*, termasuk penggunaan wajah selebriti perempuan pada konten pornografi. Otoritas penyiaran Korea juga secara rutin melakukan penghapusan massal konten *deepfake* ilegal dari internet.

Selain sanksi pidana yang diperketat, pemerintah juga gencar mengadakan kampanye literasi digital untuk meningkatkan kesadaran publik. Fokusnya adalah melindungi perempuan dan anak-anak sebagai kelompok paling rentan. Kombinasi regulasi ketat dan penegakan hukum yang konsisten menjadikan Korea Selatan salah satu contoh terbaik dalam menekan epidemi *deepfake* pornografi di tingkat nasional.

8. Australia

Australia belum memberlakukan undang-undang atau peraturan khusus yang secara langsung mengatur AI. Hingga saat ini, respons Australia terhadap AI bersifat sukarela, termasuk *the AI Ethics Principles* yang diterbitkan pada tahun 2019 yang terdiri dari delapan prinsip sukarela untuk desain, pengembangan, dan implementasi AI yang bertanggung jawab, yang konsisten dengan Prinsip-Prinsip OECD tentang AI.

Pada bulan Agustus 2024, Pemerintah Australia memperkenalkan *the Voluntary AI Safety Standard* yang terdiri dari sepuluh prinsip sukarela yang mencakup aspek-aspek seperti transparansi dengan organisasi lain, proses akuntabilitas, dan manajemen risiko AI. Standar ini menawarkan panduan praktis bagi organisasi Australia untuk memitigasi risiko sekaligus memanfaatkan manfaat AI, dengan memuat elemen-elemen sebagai berikut:

a. **Akuntabilitas**: Menetapkan, menerapkan, dan menerbitkan proses akuntabilitas yang menguraikan kebijakan tata kelola dan strategi kepatuhan regulasi.

b. **Manajemen Risiko**: Menetapkan dan menerapkan proses manajemen risiko untuk mengidentifikasi dan memitigasi risiko yang diketahui atau dapat diperkirakan.

c. **Tata Kelola Data**: Melindungi sistem AI dengan menerapkan tata kelola data, privasi, dan langkah-langkah keamanan siber untuk mengelola kerentanan keamanan seperti kualitas dan akses data.

d. **Pengujian Model**: Menguji model AI dan mengevaluasi kinerja sebelum menempatkan sistem AI berisiko tinggi di pasar, serta memantau sistem secara terus-menerus setelah diterapkan.

e. **Pengawasan Manusia**: Memungkinkan kontrol dan intervensi manusia di seluruh sistem AI untuk mencapai pengawasan manusia yang bermakna.

f. **Informasi Pengguna**: Menginformasikan pengguna akhir tentang bagaimana AI digunakan, terutama seputar keputusan yang didukung AI, interaksi AI, dan konten yang dihasilkan AI.

g. **Mekanisme Pengaduan**: Menetapkan proses bagi orang-orang yang terdampak negatif oleh sistem AI berisiko tinggi untuk menentang keputusan yang didukung AI atau mengajukan pengaduan tentang pengalaman mereka.

h. **Transparansi**: Bersikap transparan dengan organisasi lain di seluruh rantai pasok AI dengan berbagi informasi tentang data, model, dan sistem untuk memitigasi risiko secara efektif.

i. **Pencatatan**: Menyimpan dan memelihara data. catatan, termasuk dokumentasi teknis, untuk memungkinkan pihak ketiga menilai kepatuhan terhadap aturan

j. **Libatkan pemangku kepentingan**: Libatkan pemangku kepentingan dan evaluasi kebutuhan serta keadaan mereka, dengan fokus pada keselamatan, keberagaman, inklusi, dan keadilan.

Pada bulan September 2024 menerbitkan proposal yang memperkenalkan batasan wajib untuk AI dalam konteks berisiko tinggi.

Selain itu, terdapat sejumlah regulasi yang relevan sebagai rujukan dalam penggunaan AI, antara lain sebagai berikut:

The Online Safety Act 2021, yang mencakup mekanisme untuk mengatasi masalah keamanan daring, yang mencakup materi yang dihasilkan AI.

a. *The Australian Consumer Law*, yang diterapkan pada pengambilan keputusan algoritmik dalam kasus Pengadilan Federal yang memerintahkan Trivago untuk membayar denda sebesar $44,7 juta karena menyesatkan konsumen tentang tarif kamar dalam rekomendasi yang dibuat oleh algoritmanya.
b. *The Privacy Act 19888*
c. *The Corporations Act 20019*
d. *Intellectual property laws*, dapat memengaruhi beberapa aspek pengembangan dan penggunaan AI.
e. *Anti-discrimination laws,* misalnya, ketika seseorang menjadi korban diskriminasi yang diakibatkan oleh proses yang digerakkan oleh AI.

Secara khusus terkait penggunaan *deepfake*, Australia menangani *deepfake* melalui kombinasi hukum yang sudah ada dan regulasi baru. *The Online Safety Act 2021* memberi kewenangan besar kepada eSafety Commissioner untuk memerintahkan penghapusan konten berbahaya, termasuk *deepfake*. Selain itu, berlaku pula *the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, yang mengkriminalkan penciptaan dan distribusi *deepfake* intim tanpa persetujuan subyek datanya. Aturan ini menyasar langsung pelaku individu maupun jaringan yang memproduksi konten ilegal.

Regulasi Australia juga memberi perhatian khusus pada perlindungan anak dari eksploitasi berbasis *deepfake*. Kasus pelanggaran yang melibatkan anak di bawah umur diperlakukan dengan sanksi pidana yang lebih berat. Dengan pendekatan berbasis perlindungan konsumen digital, Australia menempatkan dirinya sebagai negara dengan regulasi yang cukup komprehensif di kawasan Pasifik.

9. Singapura

Singapura mengadopsi pendekatan *online harms* yang menekankan pencegahan kerugian digital bagi masyarakat. Melalui *the Online Criminal Harms Act (OCHA),* pemerintah memiliki kewenangan untuk memerintahkan platform menerapkan langkah teknis dalam menangkal konten *deepfake* yang digunakan untuk penipuan atau penyamaran pejabat publik. Pemerintah juga melibatkan *Singapore Police Force (SPF), Monetary Authority of Singapore (MAS),* dan *Cyber Security Agency (CSA)* untuk menangani kasus *deepfake* lintas sektor, terutama dalam konteks kejahatan finansial dan penipuan daring.

CSA secara khusus mengeluarkan panduan publik tentang cara mendeteksi dan melaporkan *deepfake*. Ini bertujuan meningkatkan kesadaran masyarakat agar tidak mudah terjebak pada konten manipulatif. Dengan regulasi yang adaptif dan kolaborasi lintas lembaga, Singapura berupaya membangun sistem respons cepat untuk mencegah dampak sistemik dari penyalahgunaan *deepfake*.

BAB
6

REGULASI YANG RELEVAN DI INDONESIA

Dalam perlindungan data biometrik, penggunaan AI, serta fenomena *deepfake*, terdapat beberapa regulasi di Indonesia yang dapat dijadikan dasar hukum, meskipun sebagian besar masih bersifat umum dan belum secara spesifik mengatur teknologi *deepfake*.

1. Kitab Undang-Undang Hukum Pidana (KUHP)

Tindak pidana penipuan diatur dalam Pasal 378 KUHPlama sampai saat ini masih berlaku dan Pasal 492 UU No. 1/2023 tentang KUHP baru.

Bunyi Pasal 378 KUHP tentang tindak pidana penipuan adalah:

"Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun."

Adapun, pasal tindak pidana penipuan dalam Pasal 492 UU 1/2023 adalah:

"Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata

bohong, menggerakkan orang supaya menyerahkan suatu barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V".

Menurut R. Sugandhi, unsur-unsur tindak pidana penipuan dalam Pasal 378 KUHP meliputi perbuatan seseorang yang menggunakan tipu daya, rangkaian kebohongan, identitas palsu, atau keadaan yang dipalsukan dengan tujuan memperoleh keuntungan pribadi secara tidak sah (Hukum Online, 2023). Apabila ditarik ke dalam konteks perkembangan teknologi saat ini, penggunaan *deepfake*—yakni manipulasi citra dan suara berbasis kecerdasan buatan untuk meniru seseorang—dapat memenuhi unsur penipuan tersebut. *Deepfake* sering kali digunakan untuk menipu publik dengan menampilkan wajah atau suara orang terkenal seolah-olah mengatakan sesuatu yang sebenarnya tidak pernah dilakukan, sehingga mendorong korban untuk melakukan suatu perbuatan yang berujung pada kerugian.

Putri, Salsabila, dan Hosnah menyoroti bahwa *deepfake* dapat *dikriminalisasi* dalam kerangka penipuan dan pencemaran nama baik, meskipun regulasi positif di Indonesia seperti UU ITE dan UU Perlindungan Data Pribadi masih belum mengatur secara eksplisit (Putri, Salsabila, & Hosnah, 2024). Penelitian lain oleh Dwiandari dan Arifin juga menegaskan bahwa penyalahgunaan identitas digital melalui *deepfake* untuk kepentingan komersial dapat menimbulkan kerugian hukum, sehingga memerlukan penerapan KUHP dan regulasi terkait. (Dwiandari & R. Arifin, 2024)

Dalam praktiknya, modus penipuan dengan *deepfake* telah muncul di Indonesia, misalnya penggunaan wajah tokoh publik untuk menipu *masyarakat* dalam tawaran bantuan uang palsu. Studi kasus ini memperlihatkan bahwa korban mudah percaya karena video menampilkan figur berwibawa yang sebenarnya hasil rekayasa teknologi. (Kristiyenda, J. Faradila, & C. Basanova, 2025) Dengan demikian, unsur nama palsu, kedudukan palsu, tipu muslihat, serta kerugian korban dalam Pasal 378 maupun Pasal 492 KUHP telah terpenuhi.

2. Kitab Undang-Undang Hukum Perdata (KUHPer)

Pasal 1365 KUHPer tentang Perbuatan Melawan Hukum. “Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut”

Penyebaran video *deepfake* merupakan salah satu contoh nyata perbuatan melawan hukum, karena pada dasarnya *deepfake* dibuat melalui manipulasi teknologi kecerdasan buatan untuk meniru wajah, suara, atau gerakan seseorang dengan tujuan yang tidak sah. Praktik ini dapat menimbulkan kerugian serius bagi korban, baik dalam bentuk materiil maupun immateriil. Kerugian materiil meliputi hilangnya peluang ekonomi, reputasi profesional, hingga potensi pendapatan yang sah akibat penyebaran konten palsu. Sementara itu, kerugian immateriil mencakup rusaknya nama baik, trauma psikologis, serta hilangnya kehormatan dan rasa aman pribadi (Ferdinal & Bakir, 2024).

Dalam perspektif hukum perdata, tindakan menyebarkan video *deepfake* memenuhi unsur perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 KUHPerdata. Perbuatan tersebut jelas dilakukan dengan kesalahan, melanggar hak subjektif orang lain—termasuk hak atas nama baik, privasi, dan kehormatan—serta bertentangan dengan kewajiban hukum. Selain itu, tindakan ini juga tidak sesuai dengan norma kesusilaan maupun kepatutan yang berlaku dalam masyarakat. Oleh sebab itu, pihak yang dirugikan memiliki hak untuk menuntut ganti rugi atas kerugian yang ditimbulkan oleh penyebaran *deepfake* (Dwiandari & Arifin, 2024).

Lebih lanjut, doktrin hukum perdata di Indonesia menegaskan bahwa perbuatan melawan hukum tidak terbatas pada pelanggaran terhadap undang-undang tertulis saja, melainkan juga mencakup tindakan yang bertentangan dengan kepatutan, kesusilaan, maupun norma sosial yang hidup dalam masyarakat (Siahaan, 2021). Oleh karena itu, penyebaran *deepfake* secara nyata memenuhi kategori perbuatan melawan hukum, karena menimbulkan kerugian baik langsung maupun tidak langsung terhadap korban. Dengan demikian, pemanfaatan *deepfake* secara ilegal harus dipandang sebagai pelanggaran serius yang menuntut pertanggungjawaban hukum, termasuk pemberian ganti rugi bagi korban (Putri, Salsabila, & Hosnah, 2024).

3. Undang-Undang No. 1 Tahun 2024 Tentang Perubahan Kedua Atas UU No. 1 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (UU ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui **UU No. 19 Tahun 2016** dan **UU No. 1 Tahun 2024**, merupakan regulasi utama yang mengatur berbagai aspek penggunaan teknologi digital di Indonesia. UU ini pada dasarnya dirancang untuk menyesuaikan perkembangan teknologi informasi, komunikasi, dan transaksi elektronik, sekaligus memberikan payung hukum bagi perlindungan masyarakat dari berbagai bentuk penyalahgunaan teknologi (Auli, 2023).

Dalam hal *AI dan deepfake*, UU ITE menjadi sangat relevan meskipun tidak secara eksplisit menyebut istilah tersebut. *Deepfake* yang menghasilkan konten manipulatif, baik berupa video, audio, maupun gambar sintetis, dapat masuk ke dalam kategori pelanggaran yang diatur UU ITE, terutama terkait penyebaran informasi elektronik yang bersifat merugikan, menyesatkan, atau melanggar norma hukum.

Pada **Pasal 27 ayat (1)** melarang distribusi atau pembuatan konten bermuatan asusila. Ketentuan ini sangat relevan untuk menjerat praktik **non-consensual intimate** *deepfake*, yaitu konten pornografi yang dibuat dengan memanfaatkan wajah atau tubuh seseorang tanpa persetujuan. Fenomena ini menjadi salah satu bentuk penyalahgunaan *deepfake* yang paling banyak ditemukan, dengan korban mayoritas perempuan dan anak (SIP Law Firm, 2025).

Selain itu **Pasal 27 ayat (3)** juga mengatur larangan perbuatan pencemaran nama baik melalui media elektronik. Manipulasi video atau audio menggunakan *deepfake* untuk menjatuhkan reputasi seseorang dapat dikualifikasikan sebagai pencemaran nama baik. Misalnya, pembuatan *deepfake* tokoh publik yang berisi pernyataan palsu atau perilaku tidak senonoh, sehingga merusak reputasi individu maupun kepercayaan masyarakat.

Pasal 28 ayat (1) mengatur larangan penyebaran berita bohong, menyesatkan, atau menimbulkan kerugian bagi konsumen dan kerusuhan di masyarakat. *Deepfake* yang diproduksi untuk tujuan **disinformasi politik** atau **penipuan finansial** masuk ke dalam kategori ini, karena dapat memicu keresahan, konflik, bahkan mengancam stabilitas demokrasi.

Larangan perbuatan terkait pengubahan, perusakan, atau manipulasi terhadap informasi elektronik juga diatur pada **Pasal 32 ayat (1) dan Pasal 35**. Konten *deepfake* pada dasarnya adalah bentuk manipulasi informasi elektronik melalui algoritma AI. Dengan demikian, pasal ini memberikan dasar hukum untuk menindak pelaku pembuat atau penyebar *deepfake* yang menyesatkan.

Serta **Pasal 51** yang memuat ketentuan pidana terhadap pelanggaran yang diatur dalam UU ITE, termasuk pidana penjara dan denda yang signifikan. Hal ini menjadi dasar penegakan hukum bagi aparat ketika menemukan kasus *deepfake* yang menimbulkan kerugian nyata, baik bagi individu maupun masyarakat luas.

Dengan kerangka hukum tersebut, UU ITE sebenarnya sudah menyediakan dasar untuk mengatur berbagai bentuk kejahatan berbasis teknologi digital, termasuk *deepfake*. Namun, sifat pengaturan UU ITE cenderung **reaktif** atau sering disebut dengan *firefighter logic*, yaitu baru dapat digunakan setelah kerugian atau pelanggaran terjadi. UU ini belum memiliki mekanisme preventif yang komprehensif, misalnya terkait kewajiban platform digital untuk mendeteksi, menandai (*labeling*), atau menghapus konten *deepfake* secara proaktif sebelum menyebar luas (Syailendra, 2025).

UU ITE sering dikombinasikan dengan regulasi lain seperti **UU TPKS** (untuk melindungi korban konten intim non-konsensual) dan **UU PDP** (untuk melindungi data biometrik). Namun, tantangan penegakan hukum tetap besar karena sulitnya identifikasi pelaku *deepfake* yang sering beroperasi secara anonim atau lintas yurisdiksi.

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

Merupakan instrumen hukum utama yang mengatur tata kelola data pribadi di Indonesia. Kehadiran UU ini menandai tonggak penting karena untuk pertama kalinya Indonesia memiliki payung hukum komprehensif yang mengatur hak-hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme pengawasan dan sanksi. Dalam perkembangan teknologi kecerdasan buatan (AI) dan fenomena *deepfake*, keberadaan UU PDP menjadi sangat relevan karena salah satu jenis data yang paling rentan dimanfaatkan dalam pembuatan *deepfake* adalah **data biometrik**, seperti wajah, suara, sidik jari, dan ekspresi tubuh (Jayanti, 2025).

UU PDP secara eksplisit mengkategorikan **data biometrik sebagai data pribadi spesifik**. Hal ini ditegaskan dalam **Pasal 4 ayat (2)** yang menyebutkan bahwa data biometrik termasuk dalam kategori data yang memerlukan tingkat pelindungan lebih tinggi dibanding data pribadi biasa. Pengakuan ini penting karena data biometrik memiliki sifat unik: permanen, tidak dapat diubah, serta melekat pada identitas individu. Sekali data biometrik bocor atau dimanfaatkan tanpa izin, kerugiannya bersifat jangka panjang dan sulit dipulihkan.

Pasal 20 dan 21 UU PDP menegaskan pentingnya persetujuan eksplisit (explicit consent) dalam setiap kegiatan pemrosesan data pribadi, termasuk data biometrik. Artinya, setiap pemrosesan data biometrik oleh perusahaan teknologi, platform digital, atau pihak lain, hanya dapat dilakukan jika ada persetujuan yang jelas, spesifik, dan diberikan secara sadar oleh subjek data. Ketentuan ini sekaligus menjadi tameng hukum bagi masyarakat agar tidak sembarangan datanya dimanfaatkan untuk kepentingan komersial ataupun manipulatif, misalnya untuk melatih model AI yang berpotensi menghasilkan konten *deepfake*.

UU PDP juga memperkenalkan konsep penting berupa *Data Protection Impact Assessment (DPIA)* sebagaimana diatur dalam **Pasal 34**. DPIA diwajibkan bagi setiap kegiatan pemrosesan data yang memiliki risiko tinggi terhadap hak dan kebebasan subjek data. Pemanfaatan teknologi AI, termasuk dalam konteks pembuatan atau deteksi *deepfake*, jelas termasuk kategori berisiko tinggi, sehingga secara hukum wajib dilakukan penilaian

dampak pelindungan data sebelum aktivitas tersebut dilaksanakan. Melalui mekanisme ini, diharapkan setiap institusi dapat mengidentifikasi potensi risiko sejak awal, serta merancang langkah mitigasi yang memadai.

Selain itu, **Pasal 51** UU PDP mengatur kewajiban bagi pengendali data tertentu untuk menunjuk *Data Protection Officer (DPO)*. Peran DPO menjadi krusial dalam konteks teknologi canggih seperti AI dan *deepfake*, karena DPO bertugas memastikan bahwa seluruh proses pengumpulan, pengolahan, dan penyimpanan data, khususnya data biometrik telah sesuai dengan prinsip pelindungan data pribadi. Dengan adanya DPO, akuntabilitas institusi dalam mengelola data sensitif menjadi lebih jelas dan dapat dipertanggungjawabkan (Yulianti, 2025).

Pasal 65 ayat (3) mengatur bahwa *setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau pihak lain, atau dapat merugikan pemilik data pribadi*. Praktik memperoleh foto, video, atau rekaman suara seseorang tanpa izin (misalnya dari media sosial) untuk dijadikan bahan *training data deepfake* jelas termasuk pelanggaran pasal ini. Pelaku *deepfake* sering mengunduh foto publik figur atau individu biasa untuk memproduksi konten manipulatif, yang dapat menimbulkan kerugian reputasi atau psikologis bagi korban (Noerman & Ibrahim, 2024).

Pasal 66 mengatur larangan bagi setiap orang untuk *secara melawan hukum mengungkapkan data pribadi yang bukan miliknya*. Dalam *deepfake*, ketika pelaku menyebarkan hasil manipulasi (misalnya konten intim non-konsensual) berbasis data biometrik seseorang, maka tindakan tersebut dapat dikualifikasikan sebagai *pengungkapan data pribadi tanpa hak*. Hal ini memperluas perlindungan tidak hanya pada tahap pengambilan data, tetapi juga pada tahap distribusi hasil *deepfake*.

Pasal 67 ayat (3) mengatur bahwa *setiap orang dilarang menggunakan data pribadi yang bukan miliknya dengan cara apa pun yang dapat merugikan pemilik data pribadi*. Pembuatan *deepfake* berbasis wajah atau suara jelas merupakan "penggunaan data pribadi" tanpa hak. Misalnya, manipulasi wajah selebriti atau politisi dalam video pornografi atau ujaran politik palsu dapat merugikan secara psikologis, finansial, dan reputasi. Pasal

ini menjadi dasar hukum untuk menindak pelaku yang memanfaatkan data biometrik korban untuk tujuan merugikan.

Pasal 68 juga mengatur larangan bagi setiap orang untuk *memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan orang lain*. Konten *deepfake* pada hakikatnya adalah pemalsuan data pribadi wajah, suara, atau tubuh seseorang untuk tujuan tertentu. Baik digunakan dalam modus penipuan (*scam deepfake*) maupun pembuatan konten asusila non-konsensual, tindakan ini dapat dijerat dengan Pasal 68 karena termasuk dalam kategori pemalsuan data pribadi yang merugikan korban.

Dengan kerangka hukum ini, UU PDP memberikan fondasi penting bagi Indonesia dalam menghadapi tantangan era digital, khususnya ancaman penyalahgunaan data biometrik oleh teknologi AI seperti *deepfake*. Namun, tantangan implementasi masih besar, terutama karena pengaturan teknis melalui peraturan pemerintah (PP) dan peraturan menteri (Permen) masih dalam tahap penyusunan, serta kesadaran masyarakat mengenai hak-haknya sebagai subjek data masih relatif rendah.

BAB
7

MITIGASI RISIKO, DAMPAK SOSIAL, DAN PENTINGNYA LITERASI DIGITAL

1. Mitigasi Risiko dengan DPIA Spesifik *Deepfake*

Perkembangan teknologi AI yang mampu memanipulasi data biometrik melalui teknik *deepfake* ini menghadirkan tantangan serius terhadap keamanan di tingkat individu hingga di tingkat global. Oleh karena itu, diperlukan merancang suatu mekanisme pencegahan sistematis melalui Data Protection Impact Assessment (DPIA) dengan secara spesifik untuk mengantisipasi risiko penggunaan teknologi *deepfake* tersebut.

DPIA ini sangat penting karena karena menjadi instrumen strategis dalam memastikan pemrosesan data biometrik berbasis AI tidak menimbulkan kerugian yang lebih besar dibandingkan dengan manfaatnya. Dengan melakukan asesmen sejak awal, berbagai pihak dapat mengidentifikasi celah risiko, memprediksi potensi penyalahgunaan, serta merancang langkah mitigasi sebelum insiden keamanan benar-benar terjadi.

Beberapa tahapan penting yang dapat dilakukan dalam pelaksanaan DPIA spesifik *deepfake* ini:

a. Mengidentifikasi tujuan atau alasan penggunaan data biometrik, misalnya apakah untuk kebutuhan otentikasi identitas, keamanan transaksi, atau kebutuhan analitik.

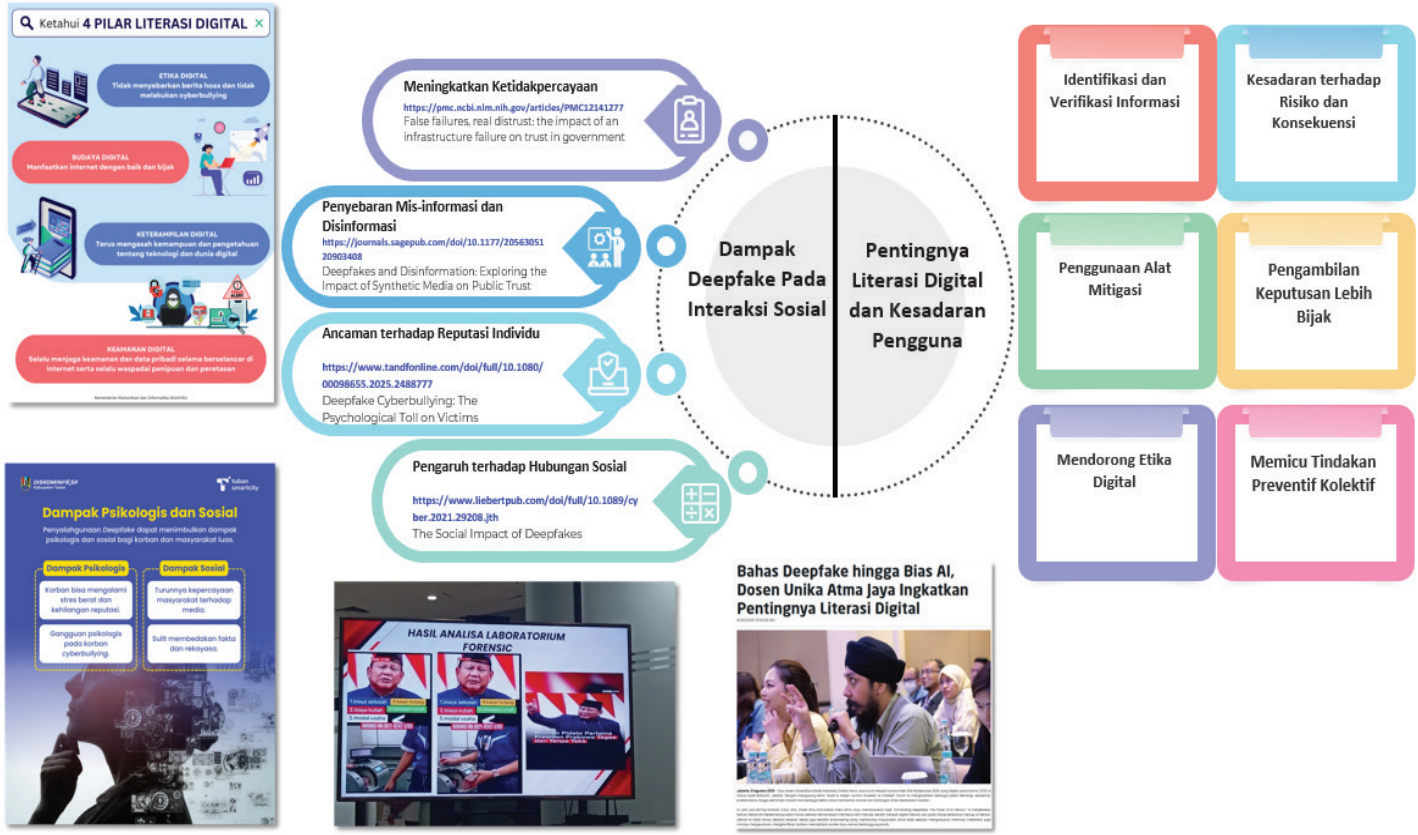
b. Mengidentifikasi risiko dengan mengkaji semua kemungkinan terjadi penyalahgunaan data biometrik seperti pencurian identitas, menembus sistem autentikasi, manipulasi video dan suara, atau berbagai risiko lainnya.
c. Menganalisis semua dampak kerugian yang dapat terjadi dari setiap risiko tersebut, baik pada tingkat individu, organisasi, masyarakat, negara, maupun di tingkat global.
d. Merancang dan melakukan strategi mitigasi dengan solusi teknis dan kebijakan untuk menekan risiko ke level yang dapat diterima.

Strategi mitigasi secara teknis yang dapat diintegrasikan dalam DPIA untuk menghadapi risiko *deepfake*, salah satunya adalah mengecek tanda digital (watermark) dari suatu konten dan mengecek metadata untuk membantu melacak sumber asli data dan memvalidasi integritas informasi (Jiwani & Poetro, 2025; Fransiskus & P, 2024). Pemanfaatan sistem deteksi *deepfake* berbasis AI juga dapat digunakan untuk mengecek apakah suatu konten dibuat oleh campur tangan AI atau tidak, karena pada dasarnya manusia cukup sulit untuk bisa mendeteksi manipulasi visual atau suara yang dibuat oleh teknologi *deepfake* tersebut. Selain itu, adopsi pendekatan zero-trust security untuk data biometrik juga dapat diimplementasikan, dimana pendekatan keamanan ini dengan cara menganggap setiap entitas baik internal ataupun eksternal tidak aman, sehingga semua akses ke data biometrik tetap harus diverifikasi secara ketat dan berlapis (Jangid, Gupta, & Sharma, 2025).

Strategi mitigasi kebijakan melalui aspek tata kelola dalam hal ini juga menjadi sangat penting, salah satunya dengan menerapkan kewajiban transparansi pemrosesan biometrik sehingga setiap organisasi yang mengolah data biometrik harus secara penuh untuk terbuka dalam menyampaikan maksud/tujuan, metode, dan potensi risiko pemrosesan kepada penggunanya. Perlu juga untuk melakukan audit kepatuhan dan tanggung jawab hukum secaara berkala untuk dapat memastikan kepatuhan terhadap regulasi perlindungan data, serta mekanisme penegakan hukum bagi pihak yang lalai untuk melakukan penyalahgunaan tersebut. Selain itu, pembuatan dan pengembangan standar kode etik di sektor publik untuk membatasi penggunaan *deepfake* perlu dilakukan, sehingga penggunaan *deepfake* ini jelas hanya pada tujuan yang sah seperti edukasi, riset, hiburan, atau tujuan lainnya yang tidak merugikan pihak lain.

2. Dampak Teknologi *Deepfake* pada Interaksi Sosial

Teknologi *deepfake* tidak hanya mempengaruhi aspek keamanan data biometrik, tetapi juga dapat membawa implikasi yang lebih luas terhadap pola interaksi sosial di masyarakat. Terlihat pada Gambar 4, kehadiran teknologi ini mengubah cara setiap individu dalam berkomunikasi dan percaya terhadap suatu informasi. *Deepfake* dapat menimbulkan krisis kepercayaan setiap dalam konsumsi konten digital. Kita bisa melihat bahwa masyarakat akan semakin sulit membedakan mana informasi yang otentik dan informasi yang dimanipulasi atau dibuat oleh AI. Hal ini jika berlangsung secara terus-menerus dapat mengikis fondasi kepercayaan publik terhadap media, lembaga, maupun individu. Sehingga berpotensi mempertanyakan validitas dari setiap konten di berbagai media (Fitri, et al., 2025).



Gambar 5. Dampak *Deepfake* pada Interaksi Sosial serta Pentingnya Literasi Digital dan Kesadaran Pengguna

Pada tingkat personal, teknologi *deepfake* membuka peluang terjadi penyalahgunaan serius seperti manipulasi identitas, fitnah, bahkan konten pornografi non-konsensual. Fenomena tersebut menunjukkan bahwa *deepfake* memiliki kapasitas untuk memperburuk berbagai bentuk kekerasan berbasis gender dan pelecahan daring yang sebelumnya sudah ada. Di sisi lainnya, korban daripada teknologi *deepfake* ini kerap mengalami dampak sosial hingga psikologis yang berat seperti trauma, kecemasan, ketakutan, bahkan depresi yang berlarut-larut. Lebih jauh lagi, adanya stigma sosial membuat korban sering kali mengalami penghakiman dan pengucilan dari masyarakat sekitar (Kasita, 2022). Hal ini dapat memperburuk penderitaan korban karena harus menghadapi tekanan ganda seperti perasaan malu, dimana dampak dari psikologis korban dapat berimplikasi pada kesehatan korban yang dapat mengancam nyawanya.

Bahaya lain yang tidak kalah penting adalah kemungkinan terjadinya normalisasi konten palsu. Hal ini terjadi jika masyarakat sudah terbiasa melihat konten *deepfake* tanpa literasi digital yang memadai, maka batasan antara kebenaran dan kebohongan akan semakin kabur. Masyarakat akan menganggap bahwa konten palsu tersebut adalah sesuatu yang sudah biasa dan bahkan sah-saha saja untuk dikonsumsi maupun dibagikan. Normalisasi ini menjadi risiko yang sangat serius karena kebohongan yang ada sudah tidak lagi dianggap sebagai ancaman serius. Sebaliknya teknologi *deepfake* juga bisa digunakan seseorang untuk menutupi kebohongannya, dimana berita yang asli dianggap sebagai konten *deepfake* dan bahkan orang lain menjadi percaya pada hal kebohongan tersebut (Zahro, Fadhilah, Hermawati, Imaduddin, & Santoso, 2024).

Jika ditinjau lebih jauh, kehadiran *deepfake* dapat mengubah pola interaksi sosial dalam beberapa aspek seperti komunikasi antar individu. Beberapa orang cenderung meragukan isi pesan suara, video call, atau rekaman apapun yang diterimanya, sehingga hubungan sosial setiap orang bisa diwarnai rasa curiga yang berlebihan. Dalam lingkup komunitas, *deepfake* dapat memicu konflik, misalnya penyebaran video fitnah yang dapat memecah belah antar kelompok, organisasi, atau negara. Selain itu teknologi ini juga dapat memperlebar jurang kesenjangan digital, dimana kelompok orang yang memiliki pemahaman literasi digital akan lebih mampu melindungi diri dari berbagai ancaman risiko *deepfake*, sedangkan kelompok orang yang tidak memiliki pemahaman literasi digital yang memadai akan lebih mudah menjadi korban manipulasi.

3. Peran Literasi Digital dan Kesadaran Pengguna

Dalam menghadapi berbagai tantangan yang dibawa oleh penggunaan teknologi *deepfake* tersebut, literasi digital menjadi salah satu kunci utama sebagai alat untuk melindungi setiap individu maupun masyarakat dari dampak negatif penggunaan *deepfake*. Regulasi dan teknologi deteksi *deepfake* memang menjadi salah satu hal yang penting dalam memitigasi risiko ini, namun tanpa diiringi kemampuan kritis dari masyarakatnya untuk dapat mengenali dan menyaring informasi digital, maka kebijakan dan teknologi deteksi *deepfake* tersebut akan menjadi kurang efektif. Disini literasi digital bukan hanya sekedar kemampuan teknis seseorang dalam menggunakan perangkat digital, melainkan juga mencakup keterampilan kognitif, etis, dan sosial dalam beriteraksi di ruang digital. Literasi digital juga membantu mengurangi risiko sosial dari normalisasi konten palsu. Dengan kesadaran kolektif untuk tidak mempercayai semua informasi di media sosial, maka masyarakat akan terdorong untuk lebih selektif dan bertanggung jawab dalam mengkonsumsi ataupun membagikan konten.

Terdapat 6 indikator penting literasi digital dalam menghadapi fenomena *deepfake* ini seperti terlihat pada Gambar 5. Indikator penting tersebut sebagai berikut:

a. Identifikasi dan verifikasi informasi

Individu dengan literasi digital yang baik pastinya tidak akan mudah percaya pada video atau rekaman suara tanpa landasan bukti yang kuat. Kemampuan mendasar yang diperlukan dalam literasi digital ini adalah mengenali jenis informasi yang diterima dan melakukan verifikasi keabsahannya. Pada era *deepfake* ini, kemampuan mencakup sikap skeptis kita terhadap penilaian suatu konten visual maupun audio yang seringkali tampak terlalu sensasional. Verifikasi ini dapat dilakukan dalam berbagai cara seperti pengecekan sumber asli, membandingkan dengan berbagai media kredibel, atau menggunakan layanan fast-checking (Costaner, Lisnawita, & Guntoro, 2025).

b. Penggunaan alat mitigasi

Kita bisa melihat banyak alat anti-*deepfake* atau aplikasi untuk mendeteksi *deepfake*, reserve image search, hingga fitur pelabelan konten oleh platform digital. Kemampuan dalam memanfaatkan alat-alat bantu ini secara aktif adalah salah satu literasi digital yang dapat dilatih oleh setiap individu, sehingga bukan hanya sekedar sebagai penonton pasif konten yang tersebar di arus informasi.

c. Kesadaran terhadap risiko dan konsekuensi

Setiap individu perlu memahami bahwa penyalahgunaan data biometrik untuk *deepfake* bukan sekedar masalah teknologi, melainkan hubungan langsung dengan privasi, reputasi, bahkan keamanan diri. Kesadaran akan risiko ini membuat setiap individu untuk lebih berhati-hati dalam membagikan data biometrik mereka dalam bentuk foto, video, atau bentuk lainnya. Selain itu juga perlu pemahaman terkait konsekuensi penyebaran konten *deepfake* yang bersifat merugikan dapat menimbulkan tanggung jawab pidana maupun perdata secara hukum.

d. Pengambilan keputusan lebih bijak

Pengampilan keputusan yang bijak dalam mengkonsumsi ataupun menyebarkan informasi perlu dimiliki oleh setiap individu. Kita tidak perlu membagikan konten yang belum jelas kebenarannya, sebaliknya kita perlu mengecek lebih teliti sumber kebenaran dari konten tersebut. Selain itu, emosi perlu kita jaga supaya tidak mudah terprovokasi oleh narasi emosional yang dibalut manipulasi visual. Dengan tindakan kolektif preventif dan kebijaksanaan digital ini, maka rantai penyebaran hoaks dapat diputuskan dan pada akhirnya membentuk budaya bermedia yang lebih sehat.

e. Mendorong etika digital

Literasi digital juga mendorong etika menjadi salah satu pemahaman nilai dan tanggung jawab moral di ruang digital, dorongan ini ditujukan kepada seluruh masyarakat dan setiap individu untuk memiliki etika digital khususnya dalam menggunakan *deepfake* dengan tujuan yang tidak merugikan pihak lain. Etika digital dapat menggerakkan setiap individu dalam penggunaan teknologi *deepfake* secara positif, misalnya untuk pendidikan, seni, atau komunikasi kreatif yang tidak melanggar privasi (Tuysuz & Kılıç, 2023).

f. Memicu tindakan preventif kolektif

Kesadaran dari setiap individu dapat meluas hingga masyarakat untuk mendorong lahirnya tindakan preventif kolektif, seperti kampanye literasi, program media awareness, inisiatif dari berbagai platform digital untuk memperkuat labelisasi konten, dan berbagai tidakan lainnya. Dengan adanya dorongan untuk melakukan gerakan kolektif ini mampu memperkuat daya tahan masyarakat terhadap ancaman *deepfake* yang tidak hanya bertumpu pada individu, namun terorganisasi dalam jejaring sosial yang bekerjasama untuk saling melindungi.

Secara garis besar, untuk mewujudkan literasi digital yang baik ini dibutuhkan peran ekosistem dalam membangun kesadaran yang melibatkan berbagai pihak yaitu pendidikan formal, platform digital, masyarakat sipil, maupun pemerintah.

BAB
8

REKOMENDASI KEBIJAKAN

Dari hasil studi yang dilakukan, berikut ini dapat kami sampaikan beberapa hal sebagai rekomendasi kebijakan untuk melindungi data biometrik yang diproses dalam teknologi *deepfake*.

1. Pendekatan

Untuk menyusun suatu kebijakan untuk mengatur tata kelola pemrosesan data biometrik dalam teknologi *deepfake* oleh AI, perlu dipertimbangkan sejumlah pendekatan agar dapat menghasilkan kebijakan yang tepat guna. Kebijakan tersebut dapat dimuat dalam bungkusan regulasi yang bentuknya akan kami paparkan di bawah Angka 8.2. Adapun beberapa pendekatan yang kami usulkan untuk dipertimbangkan adalah sebagai berikut.

2. Penggunaan Prinsip-prinsip Etika, Standar, dan Regulation

Di antara sejumlah kesulitan bagi hukum untuk merespon perkembangan teknologi dengan cepat, dua di antaranya adalah bahwa kecepatan hukum untuk berubah, berkembang, atau dibentuk sering jauh tertinggal dari kecepatan inovasi. Selain itu, inovasi yang bersifat disruptif, termasuk teknologi *deepfake*, lazimnya tidak dapat diprediksi sebelumnya sehingga hukum tidak dapat atau sulit untuk mengantisipasinya dalam bentuk regulasi. Pada sisi lain, hukum tidak boleh menghambat inovasi, sehingga regulasi tidak boleh dibuat tanpa pertimbangan yang matang akan dampaknya, antara lain, bagi inovasi,

lingkungan, dan para pemangku kepentingan, termasuk bagi pelaku dan penerima manfaat atau dampaknya.

Sementara hukum bergegas untuk mengejar ketinggalan, dengan mempertimbangkan hal yang kami sampaikan di atas, maka pada tahap awal ketika pemangku kepentingan masih dalam fase mempelajari dan beradaptasi dengan suatu inovasi yang baru, seperti *deepfake*, maka dapat disusun pedoman yang memuat prinsip-prinsip etika sebagai rujukan untuk penggunaan inovasi tersebut. Dalam konteks ini, Surat Edaran Menteri Komunikasi dan Informatikan Republik Indonesia Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial tampaknya berada dalam jalur yang tepat sebagai langkah awal untuk menuju tahapan berikutnya.

Pada saat bersamaan, dapat disusun pula suatu standar untuk penggunaan teknologi *deepfake*, yang dalam konteks ini dalam bentuk pemrosesan data biometrik. Standar ini dapat membantu para pihak terkait. Sejumlah standar internasional yang relevan dapat digunakan sebagai rujukan sehingga tidak harus menyusun standar yang baru, dengan melalui proses evaluasi terlebih dahulu sebelum mengadopsinya dalam tingkat nasional. Standar internasional yang dapat disebutkan antara lain adalah ISO/IEC 2382-37:2022 - Biometrics, ISO/IEC 42001:2023 - AI Management Systems, ISO/IEC 27090 - Cybersecurity - Artificial Intelligence, ISO/IEC 27001 -Information Security Management Standard, dan ISO/IEC 27701 - Privacy Information Management System.

Pada tahapan berikutnya, dengan pemahaman yang lebih baik tentang suatu inovasi teknologi baru dan dampak penggunaannya, maka dapatlah disusun regulasi yang memuat ketentuan yang lebih spesifik, misalnya dalam konteks ini adalah pemrosesan data biometrik dalam teknologi *deepfake*. Pendekatan dengan pentahapan ini dapat dilihat telah dilakukan misalnya oleh Australia yang memulai dengan *the AI Ethics Principles* pada tahun 2019 kemudian beranjak ke tahapan berikutnya dengan diberlakukannya *The Voluntary AI Safety Standard* tahun 2024, dan berproses untuk penyusunan regulasi dengan tetap menggunakan rujukan regulasi yang relevan dan menyusun aturan spesifik untuk hal yang mendesak misalnya *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, yang mengkriminalkan penciptaan dan distribusi *deepfake* intim tanpa persetujuan subyek datanya, dengan perhatian khusus pada pengguna rentan seperti anak di bawah umur.

3. *Self-*, *Co-*, dan *State-Regulation*

Manakala regulasi yang dibuat oleh negara *(state-regulation)* belum dapat mengakomodasi kebutuhan di dalam masyarakat, sering terjadi bahwa industri beradaptasi lebih cepat dengan situasi ini melalui *self-regulation*. Cohen dan Sundararajan (2017) mendefinisikan regulasi mandiri sebagai 'realokasi tanggung jawab regulasi kepada pihak selain pemerintah.' Desentralisasi regulasi secara praktis bermanfaat, terutama dengan perkembangan pasar digital, ketika inovasi terjadi di bidang atau sektor yang belum diatur oleh regulasi negara.

Self-regulation merepresentasikan bagaimana desentralisasi regulasi dilakukan oleh aktor swasta termanifestasi dalam bentuk kontrak yang menetapkan fondasi hubungan para pihak. Sebagai sebuah kontrak, keberadaannya didasarkan pada kesepakatan antara para pihak atas ketentuan-ketentuan yang ditetapkan dalam syarat dan ketentuan. Selain itu, bentuk lainnya adalah *code of conduct* dan pengadopsian standar. *Self-regulation,* namun demikian, memiliki ketika berhadapat dengan pertanyaan apakan model regulasi ini akan cukup untuk melindungi kepentingan publik. Jordan dan Hughes (2007) menjelaskan bahwa pengertian kepentingan publik dapat bervariasi tergantung pada latar belakang politik atau budaya. Seperti halnya jenis regulasi lainnya, *self-regulation* tunduk pada batasan-batasan tertentu yang membatasi ruang lingkup penerapannya. Model regulasi ini berlaku dalam batasan pasar tertentu. Oleh karena suatu kontrak hanya mengikat para pihak, maka kontrak tersebut tidak dapat diharapkan untuk mempertimbangkan kepentingan pihak ketiga manapun. Namun demikain, kepentingan publik dapat terpengaruh oleh kontrak tersebut. Dalam hal ini, intervensi negara melalui pengaturan dan pengawasan dalam bentuk *state-regulation* merupakan suatu keharusan. (Wahyuningtyas, 2019) Sebagai alternatif, *code of conduct* dan standar dapat mengacu pada rujukan yang sudah diakui secara global dan melalui proses evaluasi yang ketat sebelum pengadopsiannya.

Kehadiran negara untuk mengintervensi manakala terdapat kepentingan publik seperti di atas dapat pula dimanifestasikan dalam bentuk *co-regulation.* Model ini melibatkan kolaborasi antara negara

dengan sektor privat untuk penyusunan regulasi. *Co-regulation* biasanya merujuk pada situasi di mana industri mengembangkan dan mengelola pengaturannya sendiri, tetapi pemerintah memberikan dukungan legislatif untuk memungkinkan pengaturan tersebut ditegakkan.

Ketiga model ini dapat digunakan dalam tata kelola AI, termasuk *deepfake*, ketika memproses data biometrik. Dengan belum adanya regulasi dari negara, maka industri dapat berperan dengan menerapkan *self-regulation* dan pada saat yang sama bekerja sama dengan pemerintah untuk menggunakan pendekatan *co-regulation*. Namun demikian, hal ini tidak berarti mengeliminasi tanggung jawab negara untuk berinisitif menyusun regulasi, terutama ketika berkaitan dengan hal-hal yang melibatkan kepentingan publik, perimbangan kekuatan antara industri dengan konsumen, perimbangan antara pengendali dengan subyek data, dan hal-hal lain yang terkait dengan kepentingan kelompok rentan seperti anak di bawah umur.

4. Regulasi Berbasis Risiko vs. Berbasis Kerugian

Salah satu rujukan regulasi yang komprehensif mengenai AI adalah *the EU AI Act* dan *the Digital Service Act (DSA)* yang regulasinya berbasis pada penilaian risiko. Pendekatan ini adalah pendekatan yang dinilai rasional dan diharapkan tepat guna dengan merumuskan ketentuan berdasar pada risiko yang berpotensi timbul dari suatu hal yang diatur. Dengan demikian, diharapkan bahwa regulasi tidak bersifat *one size fits all*, tetapi didasarkan pada kebutuhan pengaturan yang terukur dengan mempertimbangkan potensi risikonya secara individual.

Sebagai bahan pertimbangan lain adalah regulasi berbasis kerugian yang nyata *(harm-based regulation)*. Alih-alih mendasarkan pada potensi risiko dari suatu perbuatan atau suatu hal yang akan diatur, suatu ketentuan dirumuskan berdasarkan pada kerugian yang nyata yang ditimbulkan dari perbuatan atau hal tersebut. Kelebihan dari model ini adalah dapat dihindarkannya beban biaya dan administrasi yang digunakan untuk mengevaluasi risiko. Namun demikian, kelemahannya adalah bahwa model regulasi ini akan mengandalkan pada proses pembuktian mengenai dampak kerugian yang benar-benar ditimbulkan termasuk hubungan kausal dengan perbuatan dan hal yang diatur. Selain itu, model ini juga akan

sulit digunakan untuk regulasi yang menekankan pada pencegahan, dan alih-alih, akan mengandalkan pada proses penindakan.

Atas pertimbangan tersebut di atas, pendekatan regulasi berbasis risiko sampai dengan saat ini masih merupakan pendekatan yang lebih tepat untuk diambil daripada pendekatan berbasis kerugian.

5. Regulasi Umum/Komprehensif vs. Sektoral atau Per Bidang Khusus

Idealnya suatu regulasi yang bersifat umum atau komprehensif akan memudahkan untuk penerapannya karena para pihak yang terkait akan mengacu pada satu regulasi pokok dan dengan demikian, membantu mencapai kepastian hukum bagi semua pihak. Namun demikian, pendekatan ini tidak selalu dapat dipilih, misalnya ketika obyek yang diatur sangat dinamis dan berpotensi menyentuh atau melibatkan aspek-aspek lain dalam waktu yang sulit diprediksi. Teknologi *deepfake* adalah salah satu contohnya. Penyusunan *the EU AI Act* dan DSA juga tidak ditempuh sekonyong-konyong. Keduanya melalui proses yang panjang dengan tahapan-tahapan perkembangan yang dapat dilihat dari sejarah pembentukannya.

Dalam hal demikian, maka penyusunan regulasi dapat dilakukan secara bertahap. Pada tahap awal, dapat dibentuk regulasi yang bersifat sektoral atau per bidang khusus. Sebagai contoh dapat dilihat proseses yang berlangsung di Amerika Serikat. Ketiadaan regulasi federal diisi dengan regulasi negara bagian dan tiap negara bagian merespon sesuai kebutuhannya. Salah satu respon yang menonjol adalah penyusunan regulasi di California. Dalam konteks inipun, negara bagian California tidak sekonyong-konyong menyusun regulasi yang bersifat komprehensif, melainkan memulai dengan regulasi untuk aspek-aspek tertentu, seperti terlihat dalam *the ELVIS Act* dan *California AI Transparency Act*. Tidak semua negara bagian menggunakan pendekatan ini, misalnya negara bagian Colorado dan *TRAIGA* di Texas yang mengadopsi pendekatan pengaturan berbasis risiko dan komprehensif seperti di Uni Eropa namun diadaptasi sesuai kebutuhan misalnya dalam batasan ruang lingkupnya.

Untuk situasi di Indonesia saat ini, mengadopsi regulasi yang bersifat umum atau komprehensif dapat saja dilakukan, namun akan membutuhkan

waktu. Untuk mengisi celah yang terbuka, maka dapat digunakan kerangka regulasi yang telah ada dalam antara lain KUHP, UU ITE, UU PDP, UU Perlindungan Konsumen, dan UU Anti Diskriminasi. Pada saat yang sama, dapat disusun regulasi yang spesifik meregulasi hal yang memiliki *feasibility* yang tinggi untuk diatur misalnya tentang ketentuan *disclosure* untuk penggunaan AI sebagai implementasi dari prinsip transparansi dan belajar dari pengalaman Australia dalam *the Deepfake Sexual Material Bill 2024*, kriminalisasi penciptaan dan distribusi *deepfake* intim tanpa persetujuan subyek datanya dan perhatian khusus pada perlindungan anak dari eksploitasi berbasis *deepfake* dapat dipertimbangkan.

6. Penyusunan: Pendekatan *Human-Centric* dan *Penta-Helix*

Pendekatan secara human-centric dalam tataran praktisnya, bermakna bahwa regulasi yang diambil berbasis pada penghargaan atas hak asasi manusia, martabat, demokrasi, kesetaraan, supremasi hukum, solidaritas, keadilan, inklusi, dan prinsip non-diskriminasi. Implikasinya antara lain adalah penghormatan atas manusia dan kemanusiaan sebagai dasar dari pengambilan keputusan untuk arah kebijakan yang akan dibuat. Implikasi berikutnya adalah dalam bentuk penghargaan dan pelindungan atas data pribadi yang merupakan bagian dari hak asasi manusia dan perlu mendapatkan perhatian khusus mengingat perannya yang signifikan dalam ekonomi digital pada satu sisi, dan semakin besarnya risiko pelanggaran, pada sisi lain, terlebih dalam penggunaan data biometrik dengan masifnya beragam inovasi untuk pengumpulan dan pemrosesan data biometrik untuk beragam tujuan. Dalam hal-hal sangat praktis, hal ini antara lain berdampak pada penghindaran atas pengambilan keputusan atas hidup individu semata-mata oleh mesin seperti dengan teknologi kecerdasan buatan tanpa adanya campur tangan dari manusia dan pemrosesan data biometrik dengan tanpa dasar yang sah demi alasan kepraktisan dan manfaat ekonomi.

Hingga saat ini belum terbentuk satu mekanisme yang sistematis untuk komunikasi dan interaksi yang memadai antar pemangku kepentingan yang terkait dengan pelindungan data biometrik. Proses pengembangan strategi regulasi yang komprehensif untuk merespon dan mempersiapkan

transformasi digital memerlukan pertukaran gagasan dan input yang luas dari semua pemangku kepentingan. Oleh karena itu, perlu pengembangan forum-forum dialog yang dapat mendorong interaksi antarpemangku kepentingan maupun interaksi antara pemangku kepentingan dengan pembuat regulasi. Pendekatan ini lebih tepat untuk digunakan daripada pendekatan tradisional secara top-down untuk penyusunan regulasi.

DAFTAR PUSTAKA

Agarwal A, Ratha N. Manipulating faces for identity theft via morphing and *deepfake*: Digital privacy. In: Handbook of Statistics. 2023.

Awotunde JB, Jimoh RG, Imoize AL, Abdulrazaq AT, Li CT, Lee CC. An Enhanced Deep Learning-Based *DeepFake* Video Detection and Classification System. Electronics (Switzerland). 2023;12(1).

Bharti M. AI Agents: A Systematic Review of Architectures, Components, and Evolutionary Trajectories in Autonomous Digital Systems. International Journal of Computer Engineering and Technology (IJCET). 2025; 16(1): 809-820.

Bodini, A., Manohar, A., Colecchia, F., Harrison, D., & Garaj, V. (2024). Envisioning the future of virtual production in filmmaking: A remote co-design study. Multimedia Tools and Applications, 83(7), 19015-19039.

Bunyamin JB. AGI (Artificial General Intelligence): Peluang Indonesia Melompat Jauh ke Depan. Jurnal Sistem Cerdas. 2018; 1(2): 1-11.

Chawki, M. (2024). Navigating legal challenges of *deepfake*s in the American context: a call to action. Cogent Engineering, 11(1), 123-135.

Chen, Y., Haldar, N. A., Akhtar, N., & Mian, A. (2023). Text-Image Guided Diffusion Model for Generating *Deepfake* Celebrity Interactions. arXiv, 2309, 14751. doi:https://doi.org/10.48550/arXiv.2309.14751

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107(12), 1753-1765.

Cohen, M., & Sundararajan, I. (2017). Self-regulation and innovation in the peer-to-peer sharing economy. University of Chicago Law Review Online, 82, 116–133.

Costaner, L., Lisnawita, & Guntoro. (2025). Pelatihan Literasi Digital dan Deteksi Informasi Palsu dengan Bantuan Artificial Intelligence (AI) di Sekolah. J-COSCIS : Journal of Computer Science Community Service, 5(2), 318-328. doi:https://doi.org/10.31849/6bq6jc91

Dwiandari, A. S. & R. Arifin (2024). "Criminal Law Enforcement on Digital Identity Misuse in AI Era for Commercial Interests in Indonesia," The Indonesian Journal of International Clinical Legal Education, 7(1), 80–88,

Ferdinal, O.& H. Bakir (2024). "Legal Protection Efforts and Policies to Combat *Deepfake* Porn Crimes with Artificial Intelligence (AI) in Indonesia," Journal of Multidisciplinary Sustainability Asean, (1(6), 465–474,

Fernandes YA, Fatma Y. Metode Deep Learning dalam Teknologi *Deepfake* : Systematic Literature Review. JATI (Jurnal Mahasiswa Teknik Informatika). 2025; 9(2): 3403-3410.

Fitri, D., Hidayah, A. N., Putri, A., Tanjung, N. H., Izzati, S., Ramadhani, . . . Zikri, M. (2025). *Deepfake* Dan Krisis Kepercayaan: Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial. JIIC: Jurnal Intelek Insan Cendekia, 2(6), 11556-11568. doi:https://jicnusantara.com/index.php/jiic/article/view/3787

Fransiskus, M., & P, N. (2024). Analisis Digital Forensik Metadata pada Rekayasa Digital Image sebagai Barang Bukti Digital. Jurnal InFact Sains dan Komputer, 8(1), 1-5. doi:https://doi.org/10.61179/jurnalinfact.v8i01.439

Glick, J. (2023). *Deepfake* satire and the possibilities of synthetic media. Afterimage, 50(3), 81-107.

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27(2), 27-38.

Graef, I, Wahyuningtyas, SY, Valcke, P. Assessing Data Access Issues in Online Platforms. Telecommunications Policy. 2015; 39(5), 375-387.

He J, Zhang C, Liu X, Zhang D. Survey of Research on Multimodal Fusion Technology for Deep Learning. Jisuanji Gongcheng/Computer Engineering. 2020;46(5).

Heidari A, Jafari Navimipour N, Dag H, Unal M. *Deepfake* detection using deep learning methods: A systematic and comprehensive review. Vol. 14, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2024.

Hosny, Y., & Mahfouz, M. (2025). Smart Access: Integrating Facial and Voice Biometrics with AI-Driven *Deepfake* and Spoofing Mitigation. Journal of Computing and Communication, 4(2), 62-78. doi:https://doi.org/10.21608/jocc.2025.446642

Hölbl M, Kežmah B, & Kompara M. Data protection heterogeneity in the european union. Applied Sciences (Switzerland), 2021; 11(22): 1-9. https://doi.org/10.3390/app112210912

Iyer AP, Karthikeyan J, Khan RH, Binu PM. An analysis of artificial intelligence in biometrics-the next level of security. Vol. 7, Journal of Critical Reviews. 2020.

Jangid, M., Gupta, S., & Sharma, S. (2025). Zero Trust Biometric Attendance: A Secure Face Recognition Framework. World Journal of Advanced Engineering Technology and Sciences, 15(2), 2437-2449. doi:https://doi.org/10.30574/wjaets.2025.15.2.0807

Jiwani, F. A., & Poetro, B. S. (2025). Sistem Deteksi Gambar *Deepfake* Menggunakan CNN Densenet-121 dengan Watermarking Least Significant Bit (LSB). Jurnal Rekayasa Sistem Informasi dan Teknologi, 2(3), 1157-1170. doi:https://doi.org/10.70248/jrsit.v2i3.1939

Jordan, C., & Hughes, P. (2007). Which way for market institutions: The fundamental question of self-regulation. Berkeley Business Law Journal, 4, 205–226.

Kasita, I. D. (2022). *Deepfake* Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. Jurnal Wanita dan Keluarga, 3(1), 16-26. doi:https://doi.org/10.22146/jwk.5202

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). *Deepfake*s: Trick or treat? Business horizons, 63(2), 135-146.

Khusna IH, Pangestuti S. *Deepfake*, Tantangan Baru Untuk Netizen. PROMEDIA. 2019; 5(2): 1-24.]

Kira, B. (2024). When non-consensual intimate *deepfake*s go viral: The insufficiency of the UK Online Safety Act. Computer Law & Security Review, 54(3), 106-115.

Klusch M, Lässig J, Müssig D, Macaluso A, Wilhelm FK. Quantum Artificial Intelligence: A Brief Survey. Technical Contribution. 2024; 38: 257–276.

Kristiyenda, Y. S., J. Faradila, & C. Basanova (2025). "Pencegahan Kejahatan *Deepfake*: Studi Kasus terhadap Modus Penipuan *Deepfake* Prabowo Subianto dalam Tawaran Bantuan Uang," ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 3(2).

Kshetri, N. (2023). The economics of *deepfake*s. Computer, 56(08), 89-94.

Kugler MB, Pace C. *Deepfake* privacy: Attitudes and regulation. Northwest Univ Law Rev. 2021;116(3).

Kusnadi, S. A., & Putri, D. W. (2025). Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi *Deepfake* di Indonesia. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 14(2), 195-210. doi:https://dx.doi.org/10.33331/rechtsvinding.v14i2.2135

Lees, D. (2024). *Deepfake*s in Documentary Film Production: Images of Deception in the Representation of the Real. Studies in Documentary Film, 18(2), 108-129. doi:https://doi.org/10.1080/17503280.2023.2284680

Maddocks, S. (2020). 'A *Deepfake* Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political'deep fakes. Porn Studies, 7(4), 415-423.

Maghrabi, L. A. (2025). Design of Artificial Intelligence-Based Biometric Authentication System using *Deepfake* Detection Model for Patient Data Privacy Protection and Identity Verification. Journal of Cybersecurity and Information Management (JCIM), 16(1), 269-281. doi:https://doi.org/10.54216/JCIM.160119

Mirsky, Y., & Lee, W. (2021). The creation and detection of *deepfake*s: A survey. ACM computing surveys (CSUR), 54(1), 1-41.

Mutmainnah A, Suhandi AM, Herlambang YT. Problematika Teknologi *Deepfake* Sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. UPGRADE: Jurnal Pendidikan Teknologi Informasi. 2024; 1(2): 67-72.

Noerman, C.T., A.L. Ibrahim (2024) "Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Perlindungan Negara", Jurnal USM Law Review, 7(2).

Noval, S. M. (2019). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi : Penggunaan Teknik *Deepfake*. Seminar Nasional Hasil Penelitian & Pengabdian Kepada Masyarakat (SNP2M), 4, 13-18. doi:https://jurnal.poliupg.ac.id/index.php/snp2m/article/view/1905

Nurdin, S. W., & Nugraha, I. F. (2025). Ancaman *Deepfake* dan Disinformasi Berbasis AI: Implikasi Terhadap Keamanan Siber dan Stabilitas Nasional Indonesia. JIMR: Journal Of International Multidisciplinary Research, 4(1), 73-92. doi:https://doi.org/10.62668/jimr.v4i01.1551

Okeke, A. O., Nwosu, C. J., Asogwa, J., & Dada, O. (2024). Utilization of *Deepfake* Technology in the Film Industry: Analysing Al-generated performances in the Hollywood film "The Irishman" and its impact on Artistic Integrity. Scholarly Journal of Social Sciences Research, 3(6), 35-51. doi:https://doi.org/10.5281/zenodo.13989607

Parashar A, Parashar A, Abate AF, Shekhawat RS, & Rida I. Real-Time Gait Biometrics for Surveillance Applications: A Review. Image and Vision Computing, 2023; 138, 104784. doi:https://doi.org/10.1016/j.imavis.2023.104784

Pei, G., Zhang, J., Hu, M., Zhang, Z., Wang, C., Wu, Y., . . . Tao, D. (2024). *Deepfake* Generation and Detection: A Benchmark and Survey. arXiv, 2403(17881). doi:https://doi.org/10.48550/arXiv.2403.17881

Pitaloka, C. A. (2025). Penyalahgunaan Teknologi *Deepfake* untuk Konten Pornografi NonKonsesual di Indonesia. Hukum Inovatif : Jurnal Ilmu Hukum Sosial dan Humaniora, 2(2), 74-81. doi:https://doi.org/10.62383/humif.v2i2.1475

Pasham, S. D. (2023). An Overview of Medical Artificial Intelligence Research in Artificial Intelligence-Assisted Medicine. International Journal of Social Trends, 1(1), 92-111.

Putri, S. M. I., Salsabila, N., & Hosnah, A. U. (2024). Kriminalisasi Penggunaan *Deepfake* Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum. Jurnal Hukum Legalita, 6(2), 83-90.

Rana MS, Nobi MN, Murali B, Sung AH. *Deepfake* Detection: A Systematic Literature Review. IEEE Access. 2022; 10: 25494 - 25513.

Say, T., Alkan, M., & Kocak, A. (2025). Advancing GAN *Deepfake* Detection: Mixed Datasets and Comprehensive Artifact Analysis. Applied Sciences , 15(2), 923. doi:https://doi.org/10.3390/app15020923

Seveney, M. C., Wicaksono, D. B., & Soetijono, I. K. (2025). Urgensi Regulasi Terhadap Penyalahgunaan *Deepfake* Berbasis Ai (Artificial Intelligence) Pada Konten Pornografi. Jurnal Disiplin : Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda, 31(2), 97-106. doi:https://doi.org/10.46839/disiplin.v31i2.1167

Siahaan, M. A. (2021). "Perbuatan Melawan Hukum dalam Perspektif Hukum Perdata Indonesia," Jurnal Yuridis, 8(1), 35–47.

Stupp, C. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. The Wall Street Journal, 30(08), 124-135.

Surbakti, F. P. S. (2024). Pengabdian Masyarakat sebagai Narasumber dalam Webinar Ngobrol Bareng Legislator Untuk Peningkatan Kesadaran Perlindungan Data Pribadi. Jurnal Pengabdian Masyarakat Charitas, 4(02), 58-64.

Surbakti, F. P. S. (2025). INSAN education: Towards responsible internet users. Community Empowerment, 10(2), 1-12.

Tuysuz, M. K., & Kılıç, A. (2023). Analyzing the Legal and Ethical Considerations of *Deepfake* Technology. Interdisciplinary Studies in Society, Law, and Politics, 2(2), 4-10. doi:https://doi.org/10.61838/kman.isslp.2.2.2

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Vaccari, C., & Chadwick, A. (2020). *Deepfake*s and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social media+ society, 6(1), 132-145.

Van der Sloot B, Wagensveld Y. *Deepfakes*: regulatory challenges for the synthetic society. Computer Law and Security Review. 2022;46.

Wahyuningtyas, S.Y.. (2019). Self-Regulation of Online Platform and Competition Policy Challenges: A Case Study on Go-Jek. Competition and Regulation in Network Industries, 20(1), 33–53.

Wahyuningtyas SY. Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market. Journal of European Business Organization Law Review. 2017; 18(4): 785-800.

Wahyuningtyas SY. Dampak Persaingan Bisnis Platform dengan Menggunakan Sarana Privacy Policy Tying. Jurnal Negara Hukum: Membangun Hukum untuk Keadilan dan Kesejahteraan. 2023; 14(1): 85-103.

Wahyuningtyas SY. Digital Platforms Liability for Data Governance in Data-Driven Society. Research Paper. Konferensi Ilmu Sosial dan Ilmu Politik (KISIP) 2024. Diselenggarakan oleh Safer Internet Lab, CSIS Indonesia, & Google, Jakarta, 17-18 Januari 2024, 1-15. https://saferinternetlab.org/wp-content/uploads/2024/01/Sih-Yuliana-Wahyuningtyas-KISIP-PAPER-2024.pdf

Wahyuningtyas SY. Implikasi Algorithmic Decision-Making (ADM) terhadap Otonomi Subyek Data dan Legalitasnya dalam Pemrosesan Data Pribadi. Jurnal Paradigma Hukum Pembangunan. 2024; 9(2): 150-189.

Wahyuningtyas SY. Regulating algorithms in the digital market: a revisit of Indonesian competition law and policy, International Review of Law, Computers & Technology, 2023; 38:1, 21-42, DOI: 10.1080/13600869.2023.2202290

Wahyuningtyas SY, The Right to be Forgotten: Bargaining the Freedom of Information for the Right to Privacy? dalam Hooi, K.Y. and Simandjuntak, D. (Eds.), Exploring the Nexus between Technologies and Human Rights: Opportunities and Challenges in Southeast Asia, SHAPE-SEA, 2019: 39-65.

Waseem S, Abu Bakar SARS, Ahmed BA, Omar Z, Eisa TAE, Dalam MEE. *DeepFake* on Face and Expression Swap: A Review. IEEE Access. 2023;11.

Widjaja, G. (2025). *Deepfake* dan Masa Depan Kebenaran: Implikasi Etis dan Sosial. Berajah Journal, 5(2), 147-156. doi:https://doi.org/10.47353/bj.v5i2.591

Wu, H. (2025). A Research on *Deepfake* Face Detection Techniques Based on Multimodal Biometric Cross – Verification. ITM Web of Conferences, 78(02017). doi:https://doi.org/10.1051/itmconf/20257802017

Yasrab R, Jiang W, Riaz A. Fighting *Deepfake*s Using Body Language Analysis. Forecasting. 2021;3(2)

Yilmaz, B. (2024). A Comprehensive Guide to Generative Adversarial Networks (GANs) and Application to Individual Electricity Demand. (2024). Expert Systems with Applications, 250, 123851. doi:https://doi.org/10.1016/j.eswa.2024.123851

Zahra, N., Hapsari, R. A., & Safitri, M. (2024). Perlindungan Hukum Teknologi Identitas Digital melalui Sistem Verifikasi Identitas Berbasis Biometrik. Supremasi: Jurnal Pemikiran dan Penelitian Ilmu-ilmu Sosial, Hukum, & Pengajarannya, 19(1), 86-98. doi:https://doi.org/10.26858/supremasi.v19i1.51062

Zahro, A., Fadhilah, R. R., Hermawati, S. Z., Imaduddin, G. N., & Santoso, A. A. (2024). Dampak Penyalahgunaan *Deepfake* dalam Memanipulasi Visual: Menguak Potensi Infopocalypse di Era Post Truth Terhadap Asumsi Masyarakat pada Media Massa. Jurnal Kawistara: The Journal of Social Sciences and Humanities, 14(3), 401-415. doi:https://doi.org/10.22146/kawistara.98339

TIM PENULIS

Sih Yuliana Wahyuningtyas

Sih Yuliana Wahyuningtyas menyelesaikan Sarjana Hukum di Fakultas Hukum Universitas Gajah Mada, Yogyakarta, 1996. Magister Hukum dari Program Pascarasajana Universitas Padjadjaran, Bandung, 2002. Gelar Doktor Jura diperolehnya dari Fakultas Hukum Ludwig-Maximilian-University, Munich, Jerman, 2011. Sementara itu, Postdoctoral ditempuhnya di Centre for IT and IP (CiTiP) KU Leuven, Belgia (2013-2015). Penulis adalah Dosen Fakultas Hukum dan Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Katolik Indonesia Atma Jaya, Jakarta.

Stephen Aprius Sutresno

Stephen Aprius Sutresno menyelesaikan Sarjana Teknik Informatika di Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga, 2014. Magister Sistem Informasi dari Program Pascasarjana Universitas Kristen Satya Wacana, Salatiga, 2018. Penulis adalah Dosen Prodi Sistem Informasi, Fakultas Biosains, Teknologi, dan Inovasi dan Kepala Divisi Pengabdian kepada Masyarakat di Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Katolik Indonesia Atma Jaya, Jakarta.

Feliks Prasepta Sejahtera Surbakti

Penulis menyelesaikan Sarjana dan Magister Teknik Industri di Institut Teknologi Bandung. gelar *Doctor of Philosophy* (PhD) diperoleh dari The University of Queensland, Brisbane, Australia. Di tahun 2025 ini penulis menjadi *Visiting Lecturer* di Dalian Neusoft University of Information, China dan mendapatkan penghargaan *AI & Data Analytics Award* pada *The 6th Asia Pacific International Conference on Industrial Engineering and Operations Management (IEOM)* di Bali. Saat ini penulis adalah Kaprodi Teknik Industri, Universitas Katolik Indonesia Atma Jaya.

Petrus Dapet

Menyelesaikan Sarjana Filsafat Teologi di Sekolah Tinggi Filsafat Teologi Widya Sasana, Malang, 2006. Saat ini sedang menempuh pendidikan Sarjana Hukum Semester 7 di Fakultas Hukum Universitas Katolik Indonesia Atma Jaya Jakarta.

Kalistazaira Audriendiamanty

Mahasiswa Fakultas Hukum dengan peminatan Hukum Ekonomi dan Bisnis. Saat ini menempuh pendidikan Sarjana Hukum semester 7 di Fakultas Hukum Universitas Katolik Indonesia Atma Jaya, Jakarta.

Teresa Kaena Dharmanyoto

Menempuh studi Sarjana di Program Studi Sistem Informasi, Fakultas Biosains, Teknologi, dan Inovasi, Universitas Katolik Indonesia Atma Jaya. Penulis merupakan peraih Juara I Pemilihan Mahasiswa Berprestasi (*Most Outstanding Student*) tahun 2025 dan Penerima Beasiswa UNIKA Atma Jaya. Penulis memiliki minat peminatan di bidang *Artificial Intelligence* (AI) dan Keamanan Siber.

PELINDUNGAN DATA BIOMETRIK DALAM PEMROSESAN OLEH ***ARTIFICIAL INTELLIGENCE (AI)*** UNTUK TEKNOLOGI ***DEEPFAKE***

Deepfake merupakan salah satu penerapan teknologi *Artificial Intelligence* (AI) generatif yang dibuat menggunakan model *deep learning* yang memungkinkan pengenalan pola data yang kompleks, sehingga mampu mengubah, memanipulasi, bahkan membuat baru data gambar, video, atau suara yang dapat menyerupai data aslinya. *Deepfake* sering disebut sebagai teknologi rekayasa atau sintetis citra manusia yang dapat dipelajari oleh komputer. Inovasi disruptif yang diusung oleh AI dan memunculkan teknologi *deepfake* saat ini semakin cepat berkembang. Sementara itu, terdapat tantangan tersendiri dari sisi hukum. Salah satu yang menonjol adalah dampaknya terhadap privasi karena kemampuannya untuk mengubah pola interaksi antara teknologi dan manusia di luar yang selama ini dipahami dan diatur dalam perlindungan data yang ada di berbagai yurisdiksi di seluruh dunia. Secara spesifik, tantangan tersebut ada pada kemampuan untuk memproses data biometrik pengguna yang merupakan data sensitif dalam konteks pelindungan data pribadi, sementara pendeteksian pelanggaran semakin sulit. Buku ini disusun untuk menjawab bagaimana tipologi penyalahgunaan teknologi *deepfake* dengan pemrosesan data biometrik dan identifikasi dampak merugikan *(harm)* dalam penyalahgunaan teknologi *deepfake*, dan bagaimana teknologi *deepfake* berdampak pada interaksi sosial dan bagaimana literasi digital dan kesadaran pengguna berdampak pada penyalahgunaan teknologi *deepfake*.

Di antara sejumlah kesulitan bagi hukum untuk merespon perkembangan teknologi dengan cepat, dua di antaranya adalah bahwa kecepatan hukum untuk berubah, berkembang, atau dibentuk sering jauh tertinggal dari kecepatan inovasi. Selain itu, inovasi yang bersifat disruptif, termasuk teknologi *deepfake*, lazimnya tidak dapat diprediksi sebelumnya sehingga hukum tidak dapat atau sulit untuk mengantisipasinya dalam bentuk regulasi. Pada sisi lain, hukum tidak boleh menghambat inovasi, sehingga regulasi tidak boleh dibuat tanpa pertimbangan yang matang akan dampaknya, antara lain, bagi inovasi, lingkungan, dan para pemangku kepentingan, termasuk bagi pelaku dan penerima manfaat atau dampaknya. Sementara hukum bergegas untuk mengejar ketinggalan, maka dapat disusun pedoman yang memuat prinsip-prinsip etika sebagai rujukan untuk penggunaan inovasi tersebut dan dapat disusun pula suatu standar untuk penggunaan teknologi *deepfake*, yang dalam konteks ini dalam bentuk pemrosesan data biometrik. Pada tahapan berikutnya, dengan pemahaman yang lebih baik tentang suatu inovasi teknologi baru dan dampak penggunaannya, maka dapatlah disusun regulasi yang memuat ketentuan yang lebih spesifik.

Penerbit Universitas Katolik Indonesia Atma Jaya
Jl. Jend. Sudirman Kav. 51
Jakarta 12930 Indonesia
Phone : (021) 5703306 psw. 631
Email : penerbit@atmajaya.ac.id
Website : http:// www.atmajaya.ac.id

ISBN 978-634-7009-56-2 (PDF)
9 786347 009562