DEEPFAKE MENYEBAR CEPAT, HUKUM BERGERAK LAMBAT

Pertanyaannya hari ini bukan lagi apakah Indonesia perlu regulasi deepfake, melainkan kapan kita akan benar-benar bertindak. Jika kita terus menunggu hingga jumlah korbannya tak terhitung, maka kita sudah kalah bahkan sebelum perang dimulai. Di era digital, kebenaran akan dimiliki oleh mereka yang paling lihai memanipulasi piksel.

Muhammad Ilman Abidin

16 Oktober 2025

Bacaan 6 Menit

Januari 2025, Bareskrim Polri menangkap AMA di Lampung Tengah. Pelaku menggunakan video *deepfake* menampilkan wajah dan suara Presiden Prabowo Subianto seolah-olah menawarkan bantuan sosial

pemerintah. Ratusan korban dari 20 provinsi tertipu, dengan kerugian mencapai puluhan juta rupiah. AMA dijerat UU ITE dengan ancaman 12 tahun penjara dan denda Rp12 miliar.

Sebulan kemudian, Februari 2025, Polri kembali menangkap JS (25) di Pringsewu, Lampung. Kali ini pelaku memakai *deepfake* Presiden Prabowo dan Menteri Keuangan Sri Mulyani. Sejak Desember 2024, JS meraup Rp65 juta dari sekitar 100 korban di seluruh Indonesia.

April 2025, Polda Jawa Timur mengungkap kasus serupa. Tiga pelaku asal Pangandaran membuat *deepfake* Gubernur Khofifah Indar Parawansa yang seolah menawarkan sepeda motor Rp500.000 sebagai "program gubernur". Total keuntungan: Rp87 juta. Modus serupa juga menimpa Gubernur Jawa Barat dan Jawa Tengah.

Agustus 2025, video *deepfake* memotong pidato Menteri Keuangan Sri Mulyani di ITB, seolah-olah beliau menyebut "guru sebagai beban negara". Video itu viral. Sri Mulyani mengklarifikasi di Instagram bahwa video tersebut hoaks, namun terlambat, rumahnya dijarah massa pada 31 Agustus 2025. Ini bukan lagi fiksi ilmiah. Ini Indonesia, 2025.

Data yang Menunjukkan Krisis

Data PT Indonesia Digital Identity (VIDA) mencatat lonjakan kasus penipuan *deepfake* sebesar 1.550% antara 2022–2023. Kementerian Komdigi menemukan 1.923 isu hoaks sepanjang 2024. Di sektor kripto, Chainalysis dan Elliptic melaporkan peningkatan kasus penipuan *deepfake* sebesar 40% di Asia Tenggara sepanjang 2024. Tokocrypto bersama VIDA memblokir 27.000 upaya serangan siber hanya dalam lima bulan pertama 2025. Polisi kewalahan. Korban terus berjatuhan. Pelaku semakin canggih, dan yang paling menyakitkan: hukum Indonesia masih tertatih mengejar.

Pasal 27 UU ITE, Pisau Tumpul untuk Perang Modern

Pasal 27 ayat (3) UU ITE mengancam pidana bagi siapapun yang "mendistribusikan informasi elektronik yang memiliki muatan

penghinaan dan/atau pencemaran nama baik." Sekilas tampak relevan, tapi tidak.

Dalam praktik, pasal ini mensyaratkan adanya "informasi elektronik" yang berisi pernyataan faktual. Sementara *deepfake* justru menciptakan realitas sintetis yang tidak pernah terjadi. Maka timbul pertanyaan: apakah *deepfake* termasuk "informasi" atau justru "*synthetic media*" yang tak tersentuh definisi hukum? Belum ada yurisprudensi yang jelas.

Pertanyaannya hari ini bukan lagi apakah Indonesia perlu regulasi deepfake, melainkan kapan kita akan benar-benar bertindak. Jika kita terus menunggu hingga jumlah korbannya tak terhitung, maka kita sudah kalah bahkan sebelum perang dimulai. Di era digital, kebenaran akan dimiliki oleh mereka yang paling lihai memanipulasi piksel.

Pasal 28 ayat (2) tentang berita bohong juga tidak memadai. Pasal ini menargetkan ujaran kebencian, bukan penipuan finansial atau eksploitasi seksual. Akibatnya, banyak pelaku *deepfake fraud* lolos jerat hukum.

UU PDP 2022 pun tak menolong. Pasal 65 melarang pemrosesan data pribadi secara melawan hukum, tetapi definisi "data pribadi" tidak mencakup representasi sintetis wajah atau suara yang dibuat tanpa mencuri data asli. Jika seseorang membuat *deepfake* wajah Anda hanya dari 10 foto publik di Instagram tanpa peretasan, apakah itu melanggar hukum? Secara hukum: abu-abu.

Membandingkan dengan Korea yang Bergerak Cepat

September 2024, Korea Selatan mengambil langkah tegas. Parlemen di Seoul menyetujui revisi undang-undang yang tidak hanya mengkriminalisasi pembuatan dan distribusi *deepfake* pornografi non-konsensual, tetapi juga melarang kepemilikan dan penontonan konten tersebut, dengan ancaman hingga 3 tahun penjara atau

denda besar. Sementara itu, hukuman untuk pelaku pembuat dan penyebar *deepfake* pornografi dinaikkan hingga 7 tahun penjara.

Kebijakan ini menuai protes dari aktivis HAM dan pelaku industri AI yang menilai kebijakan tersebut berpotensi menekan inovasi. Namun, pemerintah Korea berdiri teguh: data menunjukkan bahwa sebagian besar korban *deepfake* pornografi adalah perempuan muda, dan dampak psikologisnya sangat berat, banyak yang mengalami trauma dan gangguan sosial serius. Dalam pandangan mereka, perlindungan martabat manusia lebih penting daripada kebebasan teknologi. Langkah itu membuahkan hasil. Dalam beberapa bulan pertama sejak undang-undang berlaku, otoritas siber Korea melaporkan peningkatan signifikan dalam jumlah penangkapan dan penutupan situs dark web yang melayani pengguna domestik.

Indonesia? Masih sibuk berdebat apakah UU ITE perlu direvisi atau dicabut. Padahal sejak 2023, *deepfake* politik sudah menyerang lewat video Presiden Jokowi yang "berpidato dalam bahasa Mandarin." Komdigi mengonfirmasi bahwa video itu hoaks hasil manipulasi digital, tetapi dampaknya sudah terlanjur luas: memicu polarisasi politik dan manipulasi opini publik di tengah suhu politik yang memanas menjelang Pemilu 2024.

Ekonomi Politik Kekosongan Hukum: Siapa yang Diuntungkan?

Pertanyaan yang jarang muncul: siapa yang diuntungkan jika Indonesia tidak punya regulasi *deepfake* yang tegas? Jawabannya, platform besar dan industri AI.

Tanpa kewajiban hukum, platform seperti TikTok, Instagram, dan *marketplace* lokal tidak perlu berinvestasi pada sistem deteksi *deepfake*. Cukup mengandalkan laporan pengguna yang lamban dan tidak efektif. Industri AI lokal pun bebas mengembangkan aplikasi *face swap* dan *voice cloning* tanpa audit atau standar etik.

Pertanyaannya hari ini bukan lagi apakah Indonesia perlu regulasi deepfake, melainkan kapan kita akan benar-benar bertindak. Jika kita terus menunggu hingga jumlah korbannya tak terhitung, maka kita sudah kalah bahkan sebelum perang dimulai. Di era digital, kebenaran akan dimiliki oleh mereka yang paling lihai memanipulasi piksel.

Ironisnya, pemerintah sendiri mulai memanfaatkan AI generatif untuk simulasi kebijakan dan kampanye publik tanpa kerangka etik yang jelas. Dalam politik hukum, ketiadaan regulasi adalah bentuk regulasi itu sendiri, yang menguntungkan pihak tertentu.

Yang Dibutuhkan Bukan Hanya UU Baru, Tapi Keberanian Politik

Kita belum butuh UU baru tentang AI. Kita butuh keberanian politik untuk menafsirkan ulang hukum yang sudah ada. Mahkamah Agung dapat mengeluarkan SEMA (Surat Edaran Mahkamah Agung) yang menegaskan bahwa *deepfake* termasuk "informasi elektronik" dalam UU ITE, sehingga pelakunya dapat dijerat Pasal 27 dan 28. Untuk *deepfake* pornografi non-konsensual, penerapan Pasal 5 UU TPKS sangat relevan sebagai bentuk kekerasan seksual berbasis elektronik.

Di sisi perdata, platform yang lalai menghapus konten *deepfake* bisa dimintai tanggung jawab berdasarkan prinsip *vicarious liability*.

Langkah ini tidak memerlukan legislasi panjang. Hanya butuh keberanian Ketua Mahkamah Agung. Dari sisi eksekutif, Komdigi dapat mengeluarkan Peraturan Menteri yang mewajibkan seluruh platform dengan pengguna di atas 1 juta untuk memiliki sistem deteksi *deepfake* dalam 12 bulan, serta mewajibkan labelisasi konten AI (*content authenticity labeling*) berbasis teknologi C2PA (*Coalition for Content Provenance and Authenticity*). Pelanggaran dapat dikenai denda administratif hingga 2% dari omzet tahunan. Kerangka hukumnya sudah ada: Pasal 40 UU ITE, UU Cipta Kerja, dan Perpres 95/2018 tentang SPBE. Yang tidak ada hanyalah *political will*.

Forensik Digital, Mimpi Indah di Atas Kertas

Banyak pihak menyarankan peningkatan kapasitas forensik digital, dan itu wajar. Namun kita harus realistis. Saat ini, estimasi internal menunjukkan bahwa jumlah analis forensik digital di Bareskrim masih terbatas dan belum mencukupi untuk kebutuhan nasional. Untuk membangun ekosistem penegakan hukum terhadap kasus *deepfake*, dibutuhkan setidaknya ratusan analis tersertifikasi internasional, misalnya sekitar 500 orang, dengan biaya pelatihan yang bisa mencapai puluhan hingga ratusan juta rupiah per orang.

Belum termasuk biaya lisensi perangkat lunak komersial untuk deteksi *deepfake* berbasis AI, yang di pasar global dapat mencapai puluhan ribu dolar Amerika per tahun. Biaya sebesar itu tentu berat jika seluruhnya dibebankan pada APBN.

Solusi yang lebih realistis adalah kemitraan publik, swasta, dan akademik. Pemerintah dapat membentuk *National Deepfake Detection Consortium* yang melibatkan Bareskrim, universitas teknik, lembaga keamanan siber, dan sektor industri. Polri dapat mengirimkan kasus untuk dianalisis, sedangkan konsorsium melakukan pemeriksaan secara pro bono atau dengan biaya terbatas. Hasil analisis yang memenuhi standar forensik, termasuk *chain of custody* dan validitas metodologis, dapat digunakan sebagai alat bukti di pengadilan.

Pertanyaannya hari ini bukan lagi apakah Indonesia perlu regulasi deepfake, melainkan kapan kita akan benar-benar bertindak. Jika kita terus menunggu hingga jumlah korbannya tak terhitung, maka kita sudah kalah bahkan sebelum perang dimulai. Di era digital, kebenaran akan dimiliki oleh mereka yang paling lihai memanipulasi piksel.

Muhammad Ilman Abidin

16 Oktober 2025

Bacaan 6 Menit

India telah memulai langkah serupa melalui *Deepfakes Analysis Unit* (DAU) yang bekerja sama dengan lembaga publik, akademisi, dan platform digital untuk mengidentifikasi serta menanggulangi konten berbasis AI yang berpotensi berbahaya. Indonesia sendiri hingga kini masih berada pada tahap diskusi dan seminar, belum pada implementasi kelembagaan yang nyata.

Meme Politik atau Propaganda Berbahaya?

Masalah paling sensitif adalah membedakan antara meme politik satir dan propaganda berbahaya berbasis *deepfake*. Misalnya, video presiden bernyanyi lagu dangdut sebagai sindiran kebijakan, apakah ini ekspresi politik sah atau pelanggaran hukum?

Di Uni Eropa, garis batas ditarik melalui kewajiban transparansi untuk konten sintetis dalam AI Act, sekaligus pengakuan atas ruang bagi karya artistik atau satir, serta perlindungan parodi dalam kerangka kebebasan berekspresi menurut putusan Mahkamah Uni Eropa (*CJEU, Case C-201/13 – Johan Deckmyn and Vrijheidsfonds VZW v. Helena Vandersteen and Others*). Jika konten dimaksudkan sebagai parodi yang tidak menipu publik seolah-olah rekaman asli, ia cenderung terlindungi. Jika dibuat agar tampak asli dan menyesatkan, ia wajib diungkapkan sebagai konten AI atau dapat melanggar aturan lain.

Korea Selatan mengambil pendekatan berbeda. Untuk *deepfake* seksual, negara ini mengkriminalkan bukan hanya pembuatan dan distribusi, tetapi juga menonton atau memiliki. Untuk masa kampanye, terdapat larangan 90 hari atas materi kampanye berbasis *deepfake*, terlepas dari pelabelan atau konteksnya. Dengan demikian, kerangka Korea lebih bersifat pelarangan tegas, bukan uji konteks atau intensi.

Untuk Indonesia, usulan *safe harbor* bisa diajukan sebagai kebijakan baru: konten yang secara eksplisit memberi label "parodi/satir" sejak awal tayangan dan tidak mengklaim keaslian memperoleh perlindungan dari kriminalisasi, sementara konten yang dibuat agar tampak asli dan menyesatkan tetap ilegal.

Hukum atau *Chaos*?

Bulan depan, entah di kota mana, akan muncul korban baru *deepfake*. Seorang pengusaha yang kehilangan uang, seorang perempuan yang wajahnya dipasang di video porno, atau seorang politisi yang difitnah dengan video palsu. Kita akan kembali prihatin, akan ada *trending topic*, diskusi panel, dan janji pejabat, lalu semua terlupakan.

Pertanyaannya hari ini bukan lagi apakah Indonesia perlu regulasi *deepfake*, melainkan kapan kita akan benar-benar bertindak. Jika kita terus menunggu hingga jumlah korbannya tak terhitung, maka kita sudah kalah bahkan sebelum perang dimulai. Di era digital, kebenaran akan dimiliki oleh mereka yang paling lihai memanipulasi piksel.

***) Muhammad Ilman Abidin, S.H., M.H.,** Dosen Fakultas Hukum Universitas Islam Bandung