

KEBIJAKAN HUKUM TERHADAP FENOMENA AI VOICE CLONING DI INDONESIA

LEGAL POLICY ON THE PHENOMENON OF AI VOICE CLONING IN INDONESIA

Dadang Rachmat, Mustofa Kamil, Erwawati, Dede Agus Sodikin, Djamal Efendi

Universitas Islam Syekh-Yusuf Tangerang

Coorespondence Email : dadangrahmatmitrapol@gmail.com

Received: 15-03-2026 | Revised: 25-03-2026 | Accepted: 05-04-2026 | Published: 09-05-2026

Abstract

The development of Artificial Intelligence (AI) technology has produced significant innovations, including AI Voice Cloning which enables replication of human voice with very high accuracy. Although this phenomenon has potential positive applications in various sectors, it also poses serious risks related to fraud, identity falsification, privacy violations, and intellectual property rights infringement. In Indonesia, specific regulations regarding AI Voice Cloning are not yet available, so handling this phenomenon relies on interpretation from various existing legal instruments. This study analyzes the relevant legal framework, jurisdictional challenges, and socio-economic implications of AI Voice Cloning using normative legal research methods and interdisciplinary approaches. The results show that Indonesian legal policy requires comprehensive development covering technical regulations, protection of voice rights as intellectual property objects, digital verification mechanisms, and harmonization with international standards. This study recommends the formation of specific regulations, strengthening law enforcement capacity, and developing an AI ethics ecosystem involving multi-stakeholders.

Keywords: *AI Voice Cloning, Artificial Intelligence, Technology Law, Privacy Protection, Intellectual Property Rights, Deepfake Audio, AI Regulation*

PENDAHULUAN

Revolusi teknologi kecerdasan buatan telah memasuki fase yang mengubah paradigma interaksi manusia dengan mesin. Salah satu inovasi yang paling menonjol dan kontroversial adalah AI Voice Cloning, teknologi yang memungkinkan pembuatan replika suara manusia yang hampir identik dengan suara asli menggunakan algoritma deep learning. Teknologi ini, yang merupakan bagian dari keluarga teknologi deepfake, telah mengalami kemajuan signifikan dalam beberapa tahun terakhir, dengan tingkat akurasi yang mencapai tingkat di mana pendengar manusia sulit membedakan antara suara asli dan suara sintesis.

AI Voice Cloning bekerja melalui proses text-to-speech (TTS) synthesis yang diperkuat dengan neural networks. Sistem ini dilatih menggunakan dataset audio suara target, yang dapat berupa rekaman singkat beberapa menit hingga beberapa jam, untuk mempelajari karakteristik unik suara tersebut termasuk pitch, tone, accent, cadence, dan speaking style. Setelah pelatihan, sistem dapat menghasilkan ucapan baru dalam suara target tersebut, bahkan dalam bahasa yang berbeda dari bahasa asli pembicara.

Potensi aplikasi AI Voice Cloning sangat luas dan beragam. Dalam sektor positif, teknologi ini dapat digunakan untuk:

- produksi media dan hiburan, seperti dubbing film, voice-over, dan pembuatan karakter virtual;
- aksesibilitas, membantu individu dengan gangguan bicara atau yang kehilangan kemampuan berbicara;
- pendidikan dan pelatihan, memungkinkan pembuatan materi pembelajaran yang dipersonalisasi;
- layanan pelanggan, mengotomatisasi interaksi suara yang lebih natural; dan

- e) preservasi bahasa dan budaya, merekam dan mereplikasi penutur bahasa yang terancam punah.

Namun, risiko dan potensi penyalahgunaan AI Voice Cloning sama signifikan dengan manfaatnya. Fenomena ini telah digunakan untuk berbagai kejahatan dan aktivitas merugikan, termasuk:

- a) penipuan telepon (vishing/voice phishing) di mana pelaku meniru suara anggota keluarga atau pejabat untuk meminta transfer uang;
- b) pemalsuan identitas dalam konteks perbankan dan verifikasi;
- c) pembuatan konten audio palsu untuk manipulasi politik, misinformasi, atau blackmail;
- d) pelanggaran hak kekayaan intelektual terhadap voice actors, musisi, dan public figures;
- e) pelanggaran privasi dan reputasi individu; serta (6) bypass sistem keamanan biometrik berbasis suara.

Di Indonesia, kasus-kasus terkait AI Voice Cloning mulai terdeteksi. Laporan dari Badan Siber dan Sandi Negara (BSSN) dan Kepolisian Republik Indonesia menunjukkan peningkatan insiden penipuan yang melibatkan replikasi suara. Meskipun data spesifik mengenai AI Voice Cloning masih terbatas karena teknologi ini relatif baru dan seringkali tercampur dengan metode penipuan konvensional, tren ini mengindikasikan perlunya perhatian serius dari pembuat kebijakan.

Kerangka hukum Indonesia saat ini belum memiliki regulasi spesifik yang mengatur AI Voice Cloning. Penanganan fenomena ini mengandalkan interpretasi dan aplikasi dari berbagai instrumen hukum yang ada, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Hak Cipta, dan Kitab Undang-Undang Hukum Pidana (KUHP). Namun, kesenjangan antara perkembangan teknologi dan kerangka hukum yang ada menciptakan ketidakpastian hukum dan potensi impunity bagi pelaku penyalahgunaan.

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah: 1) Bagaimana karakteristik teknis dan hukum dari fenomena AI Voice Cloning? 2) Bagaimana kerangka hukum yang ada di Indonesia mengatur atau dapat diterapkan terhadap AI Voice Cloning? 3) Apa saja tantangan hukum utama dalam penanganan AI Voice Cloning?

METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan interdisipliner yang mengintegrasikan aspek teknologi dan kebijakan. Metode pengumpulan data meliputi studi dokumen terhadap peraturan perundang-undangan, putusan pengadilan, literatur ilmiah, laporan teknis, dan dokumen kebijakan. Analisis data dilakukan dengan metode analisis kualitatif deskriptif-analitis dengan teknik interpretasi hukum, analisis konseptual, dan analisis komparatif.

HASIL DAN PEMBAHASAN

Karakteristik Teknis Dan Hukum Ai Voice Cloning

Aspek Teknis

AI Voice Cloning memiliki karakteristik teknis yang mempengaruhi implikasi hukumnya:

- Akurasi dan Realisme: Sistem modern dapat menghasilkan suara yang hampir tidak dapat dibedakan dari suara asli oleh pendengar manusia. Ini menciptakan risiko deception yang tinggi.
- Aksesibilitas: Teknologi ini semakin mudah diakses oleh publik umum melalui platform berbasis cloud dengan biaya yang relatif rendah. Ini democratizes kemampuan untuk membuat deepfake audio.

- **Skalabilitas:** Setelah model suara dilatih, suara sintetis dapat dihasilkan dalam jumlah besar dan dalam berbagai bahasa. Ini memungkinkan disinformasi dalam skala masif.
- **Detektabilitas:** Meskipun suara sintetis menjadi semakin realistis, metode deteksi juga berkembang. Namun, arms race antara generasi dan deteksi menciptakan ketidakpastian.
- **Cross-modal Capabilities:** AI Voice Cloning seringkali dikombinasikan dengan deepfake video untuk menciptakan konten multimodal yang sangat meyakinkan.

Klasifikasi Penggunaan

- Penggunaan AI Voice Cloning dapat diklasifikasikan berdasarkan niat dan dampaknya:
- **Penggunaan Beneficial:** Aksesibilitas, edukasi, media, preservasi budaya, layanan kesehatan, dan personalisasi.
- **Penggunaan Neutral:** Hiburan, eksperimen teknis, dan penggunaan pribadi dengan izin.
- **Penggunaan Harmful:** Penipuan, pemalsuan identitas, blackmail, pelanggaran HAKI, pelanggaran privasi, dan manipulasi politik.

Klasifikasi ini penting karena kebijakan hukum harus mampu membedakan antara penggunaan yang sah dan yang tidak sah, serta mengatur penggunaan berisiko tanpa menghambat inovasi.

Aspek Hukum yang Terkait

AI Voice Cloning melibatkan berbagai aspek hukum yang saling terkait:

- **Hak Cipta dan Hak Terkait:** Suara sebagai performa artistik dapat dilindungi oleh hak cipta atau hak terkait (neighboring rights). Voice actors, musisi, dan pembicara publik memiliki kepentingan dalam pengendalian penggunaan suara mereka.
- **Hak atas Citra Diri dan Publicity Rights:** Penggunaan suara individu untuk tujuan komersial tanpa izin melanggar hak atas citra diri.
- **Perlindungan Data Pribadi:** Voice data merupakan personal data yang sensitif, terutama karena dapat digunakan untuk biometric identification.
- **Kejahatan Siber:** Penggunaan AI Voice Cloning untuk penipuan, pemerasan, atau manipulasi merupakan tindak pidana.
- **Tanggung Jawab Platform:** Platform yang menyediakan teknologi voice cloning memiliki tanggung jawab terkait penggunaan teknologi mereka.

Kerangka Hukum Yang Ada Di Indonesia

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

UU ITE 2016 merupakan instrumen hukum utama yang mengatur aktivitas di ruang siber. Beberapa pasal yang relevan dengan AI Voice Cloning:

- **Pasal 27 ayat (3):** Melarang penyebaran informasi yang ditujukan untuk membuat citra seseorang jelek yang dapat menimbulkan kerugian atau rasa malu. AI Voice Cloning yang digunakan untuk membuat konten audio palsu yang merusak reputasi dapat dijerat dengan pasal ini.
- **Pasal 28:** Melarang penyebaran berita bohong dan menimbulkan kebencian. Konten audio palsu yang berisi informasi palsu dapat diatur oleh pasal ini.
- **Pasal 29:** Melarang penyebaran informasi yang memuat ancaman kekerasan atau menakut-nakuti orang secara melawan hukum.
- **Pasal 32:** Mengatur tentang hak cipta dalam bentuk elektronik. Perlindungan suara sebagai objek hak cipta dapat diatur melalui pasal ini.

Namun, UU ITE memiliki keterbatasan dalam mengatur AI Voice Cloning. Pasal-pasal tersebut tidak secara spesifik mengatur teknologi sintesis suara, sehingga penegakan hukum mengandalkan analogi dan interpretasi. Selain itu, pasal-pasal kontroversial seperti Pasal 27 ayat (3) dan Pasal 28 seringkali dikritik karena multitafsir dan potensial kriminalisasi.

Undang-Undang Perlindungan Data Pribadi (UU PDP)

UU PDP 2022 memberikan kerangka perlindungan data pribadi yang komprehensif. Voice data dapat dikategorikan sebagai data pribadi yang sensitif (biometric data) berdasarkan Pasal 1 angka 10 dan Pasal 47. Aspek-aspek yang relevan:

Prinsip pengolahan data: Pengolahan voice data harus memenuhi prinsip legalitas, keadilan, transparansi, dan tujuan terbatas.

Hak subjek data: Subjek data memiliki hak atas akses, koreksi, penghapusan, dan portabilitas data suaranya.

Kewajiban pengendali data: Pengendali data harus melaksanakan assessment dampak, melindungi data, dan melaporkan pelanggaran.

Sanksi: Pelanggaran UU PDP dapat dikenai sanksi administratif dan pidana.

UU PDP memberikan fondasi untuk melindungi voice data, namun tidak secara spesifik mengatur teknologi voice cloning. Implementasi UU PDP masih dalam tahap awal, dengan lembaga pengawas yang sedang dibentuk.

Undang-Undang Hak Cipta

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta memberikan perlindungan terhadap karya cipta dan hak terkait. Aspek yang relevan:

- Pasal 40: Hak cipta meliputi hak ekonomi dan hak moral. Hak ekonomi mencakup hak untuk mengumumkan, menggandakan, dan mengalihkan.
- Pasal 50: Hak terkait melindungi penampilan pelaku (performers). Voice actors dan musisi memiliki hak terkait atas penampilan suara mereka.
- Pasal 113: Sanksi pidana untuk pelanggaran hak cipta.

Namun, perlindungan hak cipta terhadap suara memiliki keterbatasan. Hak cipta melindungi ekspresi kreatif, bukan suara itu sendiri. Voice cloning yang menggunakan suara tanpa izin mungkin tidak selalu melanggar hak cipta jika tidak mereproduksi karya cipta spesifik, melainkan hanya karakteristik suara.

Kitab Undang-Undang Hukum Pidana (KUHP)

KUHP memberikan dasar untuk penanganan kejahatan yang melibatkan AI Voice Cloning:

- Pasal 378 (Penipuan): AI Voice Cloning yang digunakan untuk menipu dengan meniru suara pihak lain dapat dijerat dengan pasal ini.
- Pasal 263 (Pemalsuan): Pemalsuan surat atau dokumen dapat diperluas interpretasinya untuk mencakup dokumen elektronik dan audio.
- Pasal 310 (Pencemaran Nama Baik): Konten audio palsu yang merusak reputasi dapat diatur dengan pasal ini.
- Pasal 335 (Pengancaman): Penggunaan suara sintesis untuk mengancam dapat diatur dengan pasal ini.

KUHP yang baru (UU Nomor 1 Tahun 2023) memperbarui beberapa ketentuan terkait kejahatan elektronik, namun masih belum secara spesifik mengatur AI Voice Cloning.

Peraturan Sektor Spesifik

Beberapa peraturan sektor spesifik yang relevan:

Peraturan OJK: Mengatur penggunaan teknologi dalam industri jasa keuangan, termasuk verifikasi identitas dan keamanan transaksi.

Peraturan Bank Indonesia: Mengatur sistem pembayaran digital dan keamanannya.

Peraturan BSSN: Mengatur keamanan siber nasional dan penanganan insiden.

Peraturan Kemenkomdigi: Mengatur penyelenggaraan sistem elektronik dan konten digital.

Tantangan Hukum Dalam Penanganan Ai Voice Cloning

Tantangan Identifikasi dan Bukti

Tantangan utama dalam penanganan AI Voice Cloning adalah identifikasi dan pembuktian:

- Autentikasi audio: Bagaimana membuktikan bahwa rekaman audio adalah asli atau palsu? Teknologi deteksi deepfake masih dalam tahap pengembangan dan tidak selalu akurat.
- Chain of custody: Bagaimana menjaga integritas bukti digital dari pengumpulan hingga persidangan?
- Expert testimony: Kebutuhan akan ahli forensik digital yang dapat menjelaskan teknologi AI Voice Cloning kepada hakim dan juri.
- Burden of proof: Siapa yang harus membuktikan keaslian atau kepalsuan audio? Dalam konteks penipuan, korban mungkin kesulitan membuktikan bahwa suara yang mereka dengar adalah sintesis.
- Tantangan Yurisdiksi AI Voice Cloning seringkali melibatkan aktor dari berbagai yurisdiksi:
- Pelaku di luar negeri: Pengembang atau pengguna teknologi voice cloning mungkin berada di luar yurisdiksi Indonesia.
- Server di luar negeri: Platform voice cloning mungkin dihosting di yurisdiksi dengan regulasi yang berbeda.
- Korban di Indonesia: Korban penipuan voice cloning berada di Indonesia, namun pelaku sulit dijangkau.
- Cross-border enforcement: Kerja sama internasional dalam penegakan hukum terhadap kejahatan siber masih terbatas.

Tantangan Regulasi Teknologi

Tantangan regulasi teknologi meliputi:

- Pace of innovation: Teknologi AI berkembang jauh lebih cepat daripada proses legislasi.
- Technical complexity: Regulator mungkin tidak memiliki pemahaman teknis yang memadai untuk mengatur teknologi yang kompleks.
- Balancing act: Regulasi harus seimbang antara perlindungan dan inovasi. Regulasi yang terlalu ketat dapat menghambat pengembangan teknologi yang bermanfaat.
- Definition challenges: Mendefinisikan AI Voice Cloning dalam bahasa hukum yang tegas namun tidak terlalu sempit atau terlalu luas.

Tantangan Perlindungan Hak

Tantangan perlindungan hak meliputi:

- Freedom of expression: Regulasi AI Voice Cloning tidak boleh menghambat kebebasan berekspresi, termasuk satire, parody, dan komentar publik.

- **Right to innovation:** Pengembang teknologi memiliki hak untuk berinovasi. Regulasi tidak boleh secara sewenang-wenang membatasi pengembangan teknologi.
- **Access to technology:** Regulasi tidak boleh menciptakan barrier yang tidak proporsional terhadap akses teknologi yang bermanfaat.
- **Due process:** Tersangka pelanggaran AI Voice Cloning harus mendapatkan perlindungan due process yang memadai.

Rekomendasi utama adalah pembentukan regulasi khusus yang mengatur AI Voice Cloning:

- **Rancangan Undang-Undang AI:** Indonesia memerlukan undang-undang payung yang mengatur AI secara komprehensif, termasuk voice cloning. Undang-undang ini harus mengadopsi pendekatan berbasis risiko, dengan kewajiban yang berbeda berdasarkan tingkat risiko aplikasi.
- **Definisi teknis yang jelas:** Regulasi harus mendefinisikan AI Voice Cloning, deepfake audio, dan istilah terkait dengan cara yang teknis akurat namun fleksibel untuk adaptasi teknologi.
- **Klasifikasi risiko:** Mengklasifikasikan aplikasi AI Voice Cloning berdasarkan risiko: prohibited (penipuan, pemerasan), high-risk (verifikasi identitas, media politik), limited risk (hiburan dengan labeling), dan minimal risk (aksesibilitas, edukasi).

Rekomendasi untuk perlindungan hak suara:

- **Pengakuan hak suara:** Mengakui suara sebagai objek perlindungan hukum yang spesifik, baik sebagai bagian dari hak cipta, hak terkait, atau hak baru (voice rights).
- **Right to voice consent:** Menetapkan bahwa penggunaan suara individu untuk tujuan sintesis memerlukan consent yang eksplisit, informed, dan revocable.
- **Licensing framework:** Mengembangkan kerangka lisensi untuk penggunaan suara komersial, termasuk royalty dan revenue sharing.
- **Moral rights:** Melindungi hak moral pemilik suara, termasuk hak untuk tidak distorsi atau digunakan dalam konteks yang merendahkan.

Rekomendasi untuk mekanisme verifikasi:

- **Watermarking audio:** Mewajibkan watermarking digital pada audio sintetis untuk identifikasi. Watermark harus persistent dan sulit dihapus.
- **Labeling konten:** Mewajibkan labeling jelas untuk konten yang menggunakan AI Voice Cloning. Label harus prominent dan tidak dapat dihapus.
- **Verification infrastructure:** Mengembangkan infrastruktur verifikasi publik yang memungkinkan individu dan organisasi untuk memverifikasi keaslian audio.
- **Detection technology:** Mendukung pengembangan dan deployment teknologi deteksi deepfake audio.

KESIMPULAN

1. AI Voice Cloning merupakan fenomena teknologi yang memiliki potensi transformasional namun juga menimbulkan risiko signifikan terhadap keamanan, privasi, dan hak kekayaan intelektual. Di Indonesia, kebijakan hukum saat ini belum memadai untuk mengatur fenomena ini secara komprehensif, mengandalkan interpretasi dari berbagai instrumen hukum yang ada yang tidak secara spesifik dirancang untuk teknologi AI generatif.

2. Analisis terhadap kerangka hukum yang ada menunjukkan bahwa UU ITE, UU PDP, Undang-Undang Hak Cipta, dan KUHP memberikan beberapa dasar untuk penanganan AI Voice Cloning, namun dengan keterbatasan signifikan. Keterbatasan ini meliputi: (1) tidak adanya definisi spesifik mengenai AI Voice Cloning; (2) kesenjangan antara teknologi modern dan konsep hukum tradisional; (3) tantangan pembuktian dan identifikasi; (4) keterbatasan yurisdiksi lintas batas; dan (5) ketidakseimbangan antara perlindungan dan inovasi.
3. Perbandingan dengan yurisdiksi lain menunjukkan berbagai pendekatan yang dapat diadopsi. EU AI Act merepresentasikan pendekatan regulasi berbasis risiko yang komprehensif. Regulasi deep synthesis Tiongkok menunjukkan pendekatan kontrol-oriented yang spesifik. Pendekatan AS yang lebih terfragmentasi menunjukkan tantangan regulasi dalam sistem federal.
4. Implikasi sosial dan ekonomi AI Voice Cloning menuntut respons kebijakan yang segera dan komprehensif. Erosi kepercayaan terhadap informasi audio, risiko penipuan yang meningkat, dan disrupsi terhadap industri kreatif merupakan tantangan yang tidak dapat diabaikan. Namun, potensi positif teknologi ini dalam hal aksesibilitas, edukasi, dan inovasi juga harus dipertahankan.

DAFTAR PUSTAKA

Buku

- Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Murray, A. D. (2016). *Information Technology Law: The Law and Society* (3rd ed.). Oxford University Press.
- Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.
- Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
- Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
- Susskind, R., & Susskind, D. (2015). *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford University Press.
- Tegmark, M. (2017). *Life 3.0: Being Human in the Age of Artificial Intelligence*. Knopf.
- Warren, S. D., & Brandeis, L. D. (1890). *The Right to Privacy*. *Harvard Law Review*, 4(5), 193-220.

Jurnal Ilmiah

- Brennen, J. S., Howard, P. N., & Nielsen, R. K. (2018). *What to Do about Digital Disinformation*. Reuters Institute for the Study of Journalism.
- Chesney, R., & Citron, D. K. (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. *California Law Review*, 107, 1753-1819.
- Citron, D. K., & Franks, M. A. (2020). *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*. *UC Davis Law Review*, 55, 2229-2262.
- Edwards, L., & Veale, M. (2018). *Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You are Looking For*. *Duke Law & Technology Review*, 16, 18-84.
- Floridi, L., & Cows, J. (2019). *A Unified Framework of Five Principles for AI in Society*. *Harvard Data Science Review*, 1(1).
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

- Harris, Z. S. (2020). Deepfakes: False Pornography is Here and the Law Cannot Protect You. *Duke Law & Technology Review*, 17, 237-265.
- Kietzmann, J., & Dabirian, A. (2020). Deepfakes: On the Ethics of Synthetic Media. *Journal of Business Ethics*.
- Klonick, K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review*, 131(6), 1598-1670.
- Laidlaw, E. B. (2015). *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*. Cambridge University Press.
- Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), 754-772.
- Mittelstadt, B. D. (2019). Principles Alone Cannot Guarantee Ethical AI. *Nature Machine Intelligence*, 1(11), 501-507.
- Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701-1777.
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
- Schwartz, P. M. (2019). Global Data Privacy: The EU Way. *New York University Law Review*, 94(4), 771-818.
- Tusikov, N. (2016). *Chokepoints: Global Private Regulation on the Internet*. University of California Press.
- Veale, M., Binns, R., & Edwards, L. (2018). Algorithms That Remember: Algorithmic Harm and Data Protection Law. *Philosophical Transactions of the Royal Society A*, 376(2133), 20180083.
- Zarsky, T. Z. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Philosophy & Technology*, 29(4), 409-433.

Peraturan Perundang-undangan

- Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Indonesia. (2014). Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.
- Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik.
- Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- California. (2019). Assembly Bill No. 730 (AB 730) - Elections: deceptive audio or visual media.
- China. (2023). Provisions on the Administration of Deep Synthesis Internet Information Services. Cyberspace Administration of China.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1-88.
- European Parliament and Council. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, 1-102.
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689, 1-144.

Texas. (2019). House Bill No. 632 (HB 632) - Relating to the creation of a deepfake video to influence the outcome of an election.

United States. (2019). Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019 (DEEPFAKES Accountability Act). H.R. 3230, 116th Congress.

Laporan dan Dokumen Organisasi

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Keamanan Siber Indonesia 2023. BSSN.

European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM/2021/206 final.

High-Level Expert Group on Artificial Intelligence. (2019). Ethics Guidelines for Trustworthy AI. European Commission.

IEEE. (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. IEEE.

Kementerian Komunikasi dan Digital. (2024). Laporan Kinerja Penanganan Konten Negatif 2023. Kemenkomdigi.

OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments.

Otoritas Jasa Keuangan. (2024). Statistik Perkembangan Fintech 2023. OJK.

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.

United Nations. (2023). Global Digital Compact. UN Doc. A/RES/77/195.

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. WEF.

World Intellectual Property Organization. (2024). WIPO Conversation on Intellectual Property and Frontier Technologies. WIPO.

Sumber Elektronik dan Database

ElevenLabs. (2024). Voice AI Technology. Retrieved from <https://elevenlabs.io/>

European Commission. (2024). Artificial Intelligence Act. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

IEEE Standards Association. (2024). AI Standards. Retrieved from <https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>

Partnership on AI. (2024). Tenets. Retrieved from <https://www.partnershiponai.org/>

Resemble AI. (2024). Voice Cloning Technology. Retrieved from <https://www.resemble.ai/>

United Nations. (2023). Global Digital Compact. Retrieved from <https://www.un.org/techenvoy/global-digital-compact>