



Analisis Yuridis terhadap Fenomena Deepfake dalam Konteks Hak Privasi di Era Digital Global

Berliant Pertiwi ^{a,1}, Althea Serafim Kriswandaru ^{b,2}

^aUniversitas Sains dan Teknologi Komputer (STEKOM), Indonesia

^bUniversitas Sains dan Teknologi Komputer (STEKOM), Indonesia

¹berliant@stekom.ac.id; ²altheaserafim@stekom.ac.id

*email korespondensi: berliant@stekom.ac.id

INFORMASI ARTIKEL

Sejarah Artikel

Diserahkan

2024-03-30

Diterima

2024-04-21

Dipublikasikan

2024-04-30

Kata Kunci

Deepfake;

Data Privacy;

Digital Identity;

Legal Protection;

ABSTRAK

The rapid development of Artificial Intelligence (AI) technologies has significantly transformed digital content production, particularly through deepfake technology, which enables the creation of hyper-realistic audio-visual representations without consent. This phenomenon poses substantial threats to individual privacy and the integrity of digital identity, especially in legal systems that lack responsive regulatory frameworks. This study aims to analyze the extent to which the Indonesian legal system is equipped to protect individual privacy rights from deepfake threats and to examine regulatory models from other jurisdictions as comparative references. Employing a normative juridical approach combined with comparative legal analysis, the research reviews national laws, international regulations, academic literature, and case studies involving non-consensual synthetic content. The findings reveal that Indonesia lacks specific legal instruments addressing digital image and voice authorization. Although Law No. 27 of 2022 on Personal Data Protection and the Electronic Information and Transactions Law are in place, they do not explicitly cover digital identity manipulation. Indonesia's regulatory framework remains insufficient compared to regulations such as the European Union's General Data Protection Regulation (GDPR) and AI Act, or the United Kingdom's Online Safety Act. The study identifies five legal dimensions relevant to deepfake regulation, with three of them, including digital voice, image rights, and digital authorization, currently unregulated. This research contributes to the discourse on digital law by highlighting the urgency for regulatory reform and the recognition of digital identity as a protected legal right within Indonesia's legal system.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.

1. PENDAHULUAN

Dalam era digital yang semakin maju, teknologi kecerdasan buatan telah membawa dampak transformatif dalam berbagai aspek kehidupan, termasuk dalam produksi konten digital. Salah satu manifestasi teknologi AI yang berkembang pesat adalah deepfake, teknologi berbasis machine learning yang dapat menciptakan representasi audio-visual palsu yang sangat meyakinkan dari seseorang, tanpa persetujuan orang tersebut. Fenomena ini mengaburkan batas antara kenyataan dan manipulasi digital, menimbulkan risiko serius terhadap hak privasi individu, integritas identitas digital, serta keamanan informasi. Secara global, laporan dari ¹ mencatat peningkatan lebih dari 900% jumlah konten deepfake dari 2018 hingga 2023, dengan

¹ Deeptrace Labs, *The State of Deepfakes: Landscape, Threats, and Impact*, 2019 <<https://www.deeptracelabs.com/resources>>.

mayoritas digunakan dalam konteks eksploitasi seksual dan disinformasi politik. Salah satu kasus terkenal terjadi di Amerika Serikat pada tahun 2020 ketika video palsu Nancy Pelosi yang dimanipulasi untuk menunjukkan gangguan berbicara tersebar luas dan memicu disinformasi politik. Di Inggris, pada 2021, penipuan suara berbasis AI menyebabkan kerugian ratusan ribu dolar bagi sebuah perusahaan. Di Indonesia, tren penyebaran video deepfake yang menampilkan wajah publik figur mulai meningkat sejak 2022, namun hingga kini belum ada regulasi khusus yang menanganinya secara komprehensif. Situasi ini menunjukkan adanya ketimpangan antara kemajuan teknologi dan kerangka regulatif yang melindungi hak-hak digital warga negara.

Seiring meningkatnya prevalensi konten deepfake, sejumlah studi telah mengidentifikasi dampak seriusnya terhadap hak privasi dan keamanan digital. Studi oleh ² dan ³ menunjukkan bahwa deepfake berpotensi digunakan untuk pencemaran nama baik, pemerasan, hingga penipuan identitas digital. Sementara itu, laporan ⁴ menekankan bahwa deepfake juga digunakan dalam propaganda politik dan rekayasa sosial berskala besar. Di sisi hukum, regulasi di banyak negara masih tertinggal dari kecepatan perkembangan teknologi ini. Di Indonesia, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) belum secara eksplisit melindungi representasi digital seperti wajah dan suara dalam konteks rekayasa AI. Studi oleh ⁵ mengungkapkan bahwa mayoritas korban konten deepfake tidak memiliki jalur hukum yang efektif untuk menuntut keadilan atau mendapatkan pemulihan. Sementara di Amerika Serikat, rancangan Deepfake Accountability Act mulai dirumuskan, dan Inggris telah mengesahkan Online Safety Act yang mengatur distribusi konten sintesis non-konsensual secara eksplisit. Ini menunjukkan adanya kesenjangan antara negara yang progresif dan negara yang masih merumuskan kerangka hukumnya.

Beberapa penelitian terkait teknologi deepfake menunjukkan bahwa konten sintesis berbasis AI memiliki potensi besar dalam menciptakan disinformasi dan manipulasi opini publik. ⁶ menjelaskan bahwa deepfake dapat merusak kepercayaan terhadap bukti visual dan memperlemah sistem hukum berbasis fakta. ⁷ menekankan bahwa ancaman utama dari deepfake terletak pada aspek kecepatan distribusi dan kemampuan untuk meniru identitas digital tanpa izin. Sementara itu, ⁸ membahas dilema etika dari penggunaan teknologi ini yang tidak dibarengi dengan regulasi komprehensif. ⁹ memperluas diskusi ini dengan menyatakan bahwa teknologi deepfake merupakan salah satu contoh kegagalan sistem AI dalam menjamin keadilan informasi dan integritas data personal. Kelima penelitian ini menggambarkan bahwa ancaman teknologi

² Mekhail Mustak and others, 'Deepfakes: Deceptions, Mitigations, and Opportunities', *Journal of Business Research*, 154 (2023), p. 113368, doi:10.1016/j.jbusres.2022.113368.

³ Bart Van der Sloot and Yvette Wagenveld, 'Deepfakes: Regulatory Challenges for the Synthetic Society', *Computer Law & Security Review*, 46 (2022), p. 105716, doi:10.1016/j.clsr.2022.105716.

⁴ Stanford Internet Observatory, *SIO 2022 Annual Report*, 2022 <https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2023-01/sio2022_annual_report_v5.pdf>.

⁵ Karolina Mania, 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study', *Trauma, Violence, and Abuse*, 25.1 (2024), pp. 117–29, doi:10.1177/15248380221143772.

⁶ Maria Pawelec and Maria Mariapawelec, 'Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions', *Digital Society*, 1.2 (2022), pp. 1–37, doi:10.1007/s44206-022-00010-6.

⁷ Masabah Bint E. Islam and others, 'AI Threats to Politics, Elections, and Democracy: A Blockchain-Based Deepfake Authenticity Verification Framework', *Blockchains*, 2.4 (2024), pp. 458–81, doi:10.3390/blockchains2040020.

⁸ Lubna Luxmi Dhirani and others, 'Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review', *Sensors*, 23.3 (2023), p. 1151, doi:10.3390/s23031151.

⁹ Felipe Romero Moreno, 'Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content', *International Review of Law, Computers and Technology*, 38.3 (2024), pp. 297–326, doi:10.1080/13600869.2024.2324540.

deepfake tidak hanya teknis, tetapi juga memerlukan pemahaman multidisipliner, khususnya dalam bidang hukum dan etika digital.

Penelitian-penelitian lain juga mengkaji bagaimana sistem hukum saat ini belum sepenuhnya mampu merespons perkembangan pesat dari teknologi deepfake.¹⁰ menyatakan bahwa regulasi digital masih terfragmentasi dan sering kali tidak relevan terhadap dinamika konten sintetis berbasis AI.¹¹ menyoroti konsep privasi kontekstual sebagai landasan penting dalam memahami dampak deepfake terhadap hak individu.¹² mengusulkan pendekatan accountability-by-design dalam kerangka etika AI, untuk memastikan produsen dan distributor teknologi bertanggung jawab atas penggunaan sistem mereka. Sementara itu,¹³ menggarisbawahi pentingnya kebijakan berbasis hak asasi manusia dalam mengatur konten deepfake, terutama yang berkaitan dengan kebebasan berekspresi dan privasi. Studi-studi ini memberikan gambaran bahwa perumusan kebijakan hukum terkait deepfake tidak dapat dilepaskan dari kerangka etika dan prinsip-prinsip tata kelola teknologi digital yang inklusif.

Penelitian yang lebih fokus pada pendekatan hukum perbandingan juga telah dilakukan di berbagai negara untuk memahami bagaimana kebijakan terkait deepfake direspons secara global.¹⁴ mengkaji kebijakan anti-deepfake di Pakistan dan menemukan keterbatasan dalam perlindungan terhadap hak privasi non-konsensual.¹⁵ meneliti pendekatan Korea Selatan yang relatif lebih ketat dalam membatasi distribusi konten sintetis pornografi.¹⁶ mengulas tantangan hukum di India, termasuk tumpang tindih antara undang-undang teknologi informasi dan perlindungan privasi.¹⁷ menambahkan bahwa literasi digital masyarakat dan kejelasan hukum sangat menentukan efektivitas pengendalian konten deepfake. Di sisi lain,¹⁸ membandingkan pendekatan Amerika Serikat dan Uni Eropa, dan menemukan bahwa meskipun keduanya memiliki arah yang sama, mekanisme eksekusinya berbeda secara substansial. Penelitian-penelitian ini menunjukkan bahwa respons hukum terhadap deepfake sangat bergantung pada kesiapan negara dalam mengadaptasi instrumen hukum terhadap tantangan identitas digital baru.

Meskipun berbagai penelitian telah membahas dampak teknologi deepfake terhadap hak privasi dan integritas digital, sebagian besar masih terfokus pada pendekatan global atau konteks negara

¹⁰ Bo Nørregaard Jørgensen and Zheng Grace Ma, 'Regulating AI in the Energy Sector: A Scoping Review of EU Laws, Challenges, and Global Perspectives', *Energies*, 18.9 (2025), p. 2359, doi:10.3390/en18092359.

¹¹ Walter Matli, 'Extending the Theory of Information Poverty to Deepfake Technology', *International Journal of Information Management Data Insights*, 4.2 (2024), p. 100286, doi:10.1016/j.jjime.2024.100286.

¹² Kaya Axelsson, Claire Wigg, and Matilda Becker, 'Is Impact Out of Scope? A Call for Innovation in Climate Standards to Inspire Action Across Companies' Spheres of Influence', *Carbon Management*, 15.1 (2024), p. 2382995, doi:10.1080/17583004.2024.2382995.

¹³ Katalin Parti and Judit Szabó, 'The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe', *Laws*, 13.6 (2024), p. 67, doi:10.3390/laws13060067.

¹⁴ Ahmed Shafkat Sunvy, Raiyan Bin Reza, and Abdullah Al Imran, 'Media Coverage of DeepFake Disinformation: An Analysis of Three South-Asian Countries', *Informasi*, 53.2 (2023), pp. 295–308, doi:10.21831/informasi.v53i2.66479.

¹⁵ McGlynn Clare and Rüya Tuna Toparlak, 'The "New Voyeurism": Criminalizing the Creation of "Deepfake Porn"', *Journal of Law and Society*, 52.2 (2025), pp. 204–28, doi:10.1111/jols.12527.

¹⁶ Manjula Raghav and Sanjana Sharma Marwaha, 'Challenges and Issues in India's Legal Framework for the Right to Privacy in Cyberspace', *Fiat Justisia: Jurnal Ilmu Hukum*, 17.1 (2023), pp. 1–16, doi:10.25041/fiatjustisia.v17no1.2667.

¹⁷ Nadia Naffi and others, 'Empowering Youth to Combat Malicious Deepfakes and Disinformation: An Experiential and Reflective Learning Experience Informed by Personal Construct Theory', *Journal of Constructivist Psychology*, 38.1 (2023), pp. 119–40, doi:10.1080/10720537.2023.2294314.

¹⁸ Kristoffer Torngaard Pedersen and others, 'Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments', *Journal of Cybersecurity and Privacy*, 5.2 (2025), p. 18, doi:10.3390/jcp5020018.

maju, tanpa menelaah secara mendalam dinamika hukum di negara berkembang seperti Indonesia.¹⁹ serta²⁰ menyoroti potensi ancaman terhadap sistem hukum dan demokrasi, tetapi tidak secara eksplisit membahas tantangan di negara dengan sistem hukum yang belum adaptif. Studi oleh²¹ lebih banyak mengeksplorasi dimensi etika teknologi deepfake, namun belum mengarah pada kajian normatif hukum di tingkat nasional.²² mengusulkan pendekatan berbasis hak asasi manusia, namun konteksnya lebih banyak diterapkan di Uni Eropa dengan infrastruktur hukum digital yang sudah mapan. Penelitian oleh²³ pun meski mengangkat privasi kontekstual, belum menjangkau kompleksitas hukum terkait konten sintetis non-konsensual di negara seperti Indonesia. Kesenjangan ini memperlihatkan bahwa kajian hukum terhadap fenomena deepfake belum banyak dilakukan dalam ruang lingkup negara dengan sistem hukum yang masih berorientasi pada data pribadi secara sempit dan belum menjangkau hak identitas digital secara menyeluruh.

Lebih lanjut, belum banyak studi yang secara khusus menelaah kekosongan regulasi terkait perlindungan hukum terhadap individu dari penyalahgunaan citra dan suara digital berbasis AI.²⁴ memang meneliti pendekatan kebijakan di negara berkembang, tetapi tidak mengulas secara rinci instrumen hukum positif yang berlaku. Sementara itu, penelitian oleh²⁵ dan²⁶ yang membandingkan kerangka hukum internasional seperti GDPR dan Deepfake Accountability Act hanya memberikan gambaran umum tanpa analisis mendalam tentang kesiapan adopsi dalam konteks lokal Indonesia.²⁷ mencatat bahwa UU PDP dan UU ITE belum mencakup aspek otorisasi citra dan suara digital, tetapi belum dilengkapi dengan solusi normatif yang konkret.²⁸ juga belum menyoroti urgensi mekanisme remediasi bagi korban konten deepfake secara sistemik. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan memberikan analisis normatif terhadap perlindungan hak privasi, serta menyusun kerangka regulasi berbasis perbandingan hukum dan prinsip etika digital yang relevan dengan konteks Indonesia.

Penelitian ini bertujuan untuk menjawab pertanyaan utama: sejauh mana hukum nasional Indonesia saat ini mampu melindungi hak privasi individu terhadap ancaman yang ditimbulkan oleh konten deepfake? Selain itu, bagaimana praktik regulatif di negara lain dapat menjadi rujukan dalam merumuskan kebijakan hukum yang relevan di Indonesia? Fokus utama penelitian ini terletak pada analisis yuridis terhadap kekosongan regulasi yang ada, dengan

¹⁹ George Asimakopoulou and others, 'Impact of Information and Communication Technologies on Democratic Processes and Citizen Participation', *Societies*, 15.2 (2025), p. 40, doi:10.3390/soc15020040.

²⁰ Onur Bakiner, 'The Promises and Challenges of Addressing Artificial Intelligence with Human Rights', *Big Data and Society*, 10.2 (2023), pp. 1–13, doi:10.1177/20539517231205476.

²¹ Bruce Morley and Ionel Bostan, 'Consolidating the Role of AI in the Economy and Society: Combating the Deepfake Phenomenon Through Strategic and Normative Approaches—The Case of Romania in the EU Context', *Economies*, 13.5 (2025), p. 129, doi:10.3390/economies13050129.

²² Peter G. Kirchschlaeger, 'An International Data-Based Systems Agency IDA: Striving for a Peaceful, Sustainable, and Human Rights-Based Future', *Philosophies*, 9.3 (2024), pp. 1–22, doi:10.3390/philosophies9030073.

²³ David Ghiurău and Daniela Elena Popescu, 'Distinguishing Reality from AI: Approaches for Detecting Synthetic Content', *Computers*, 14.1 (2024), p. 1, doi:10.3390/computers14010001.

²⁴ Pasquale Marcello Falcone, 'Sustainable Energy Policies in Developing Countries: A Review of Challenges and Opportunities', *Energies*, 16.18 (2023), p. 6682, doi:10.3390/en16186682.

²⁵ Sk Tahsin Hossain and others, 'Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework', *Applied Sciences*, 14.13 (2024), p. 5501, doi:10.3390/app14135501.

²⁶ Anna Aseeva, 'Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech', *Sustainability*, 16.1 (2023), p. 228, doi:10.3390/su16010228.

²⁷ Ms Valeria Ferrari, 'The Platformisation of Digital Payments: The Fabrication of Consumer Interest in the EU FinTech Agenda', *Computer Law & Security Review*, 45 (2022), p. 105687, doi:10.1016/j.clsr.2022.105687.

²⁸ Beatriz Kira, 'When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act', *Computer Law & Security Review*, 54 (2024), p. 106024, doi:10.1016/j.clsr.2024.106024.

mempertimbangkan kompleksitas konten sintetis yang semakin canggih dan sulit dibedakan dari konten autentik. Penelitian ini juga akan menelaah bentuk perlindungan hukum yang telah diterapkan di beberapa yurisdiksi global, khususnya yang telah mengatur penggunaan dan distribusi konten deepfake secara eksplisit. Harapannya, penelitian ini dapat merumuskan kerangka yuridis yang lebih responsif terhadap perkembangan teknologi digital, sekaligus menawarkan kontribusi akademik dan praktis dalam pembentukan regulasi konten digital sintetis berbasis hak privasi. Dengan pendekatan tersebut, hasil penelitian ini diharapkan dapat memberikan dasar yang kuat bagi pembuat kebijakan dalam membentuk sistem hukum yang adaptif terhadap risiko baru dalam ruang digital, terutama yang berkaitan dengan pelanggaran privasi melalui rekayasa identitas secara non-konsensual.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yang fokus pada analisis norma hukum tertulis, seperti undang-undang dan peraturan perundang-undangan, khususnya dalam konteks fenomena teknologi deepfake. Untuk memperkaya pemahaman, digunakan pula pendekatan perbandingan hukum (comparative law) dan konseptual, yang bertujuan membedah prinsip filosofis dan etika yang mendasari regulasi terhadap konten digital sintetis. Penelitian ini bersifat deskriptif-analitis, dengan tujuan tidak hanya menjelaskan norma hukum yang berlaku, tetapi juga menilai efektivitasnya dalam menghadapi tantangan kontemporer.

Karena penelitian bersifat normatif, maka tidak menggunakan metode survei atau wawancara. Populasi dan sampel digantikan oleh bahan hukum, yaitu dokumen hukum primer (seperti undang-undang dan putusan pengadilan) serta dokumen sekunder (literatur akademik dan laporan lembaga internasional). Kriteria inklusi didasarkan pada relevansi materi terhadap isu hukum yang diteliti, seperti pengaruh deepfake terhadap hak privasi digital.

Pengumpulan data dilakukan melalui studi kepustakaan, yang mencakup pencarian sistematis terhadap regulasi, artikel ilmiah, dan studi kasus. Tiga jenis data utama adalah:

1. Peraturan, seperti UU PDP, GDPR, Online Safety Act (UK), dan Deepfake Accountability Act (AS);
2. Literatur, berupa jurnal hukum dan buku akademik terkait hukum AI dan privasi digital;
3. Studi kasus, seperti DeepNude, COMPAS, dan video deepfake Nancy Pelosi.

Sumber-sumber ini diperoleh dari basis data hukum nasional, jurnal akademik internasional (Scopus, JSTOR), serta laporan dari lembaga terpercaya seperti Stanford Internet Observatory. Hal ini memungkinkan analisis hukum dilakukan secara utuh dan berimbang.

Instrumen penelitian berupa analisis sistematis terhadap dokumen hukum menggunakan kerangka pertanyaan hukum, misalnya apakah suatu negara memiliki aturan spesifik terkait konten sintetis dan bagaimana tanggung jawab hukumnya dibandingkan dengan negara lain. Alat bantu seperti Zotero digunakan untuk manajemen referensi, dan NVivo digunakan jika diperlukan untuk pengkodean tematik.

Analisis data dilakukan dengan metode interpretasi hukum—baik gramatikal, sistematis, maupun teleologis—serta dengan pendekatan perbandingan hukum antarnegara. Selain itu, digunakan analisis tematik-konseptual untuk mengaitkan hak privasi dengan kebijakan hukum dalam konteks AI. Perbandingan ditampilkan dalam bentuk tabel yang menilai kesiapan hukum negara-negara seperti Indonesia, AS, Inggris, dan Uni Eropa dalam mengatur konten deepfake.

Kanada sedang dalam proses menyusun regulasi, menunjukkan adanya kesadaran hukum yang berkembang. Ketidakhadiran regulasi yang eksplisit di Indonesia mengindikasikan adanya celah perlindungan hukum terhadap penyalahgunaan teknologi deepfake, terutama yang bersifat non-konsensual atau manipulatif. Dengan membandingkan status regulatif antarnegara, peta ini menjadi alat bantu penting untuk memahami urgensi pembaruan hukum nasional dalam menghadapi tantangan etika dan hukum dari teknologi sintetis berbasis AI.

Sesuai dengan tujuan penelitian, hasil dikategorikan ke dalam tiga bagian utama, yaitu analisis perlindungan hukum terhadap hak privasi dari konten deepfake di Indonesia, identifikasi celah regulatif nasional, dan pemetaan pendekatan regulatif internasional sebagai bahan pembandingan. Pada konteks hukum Indonesia, ditemukan bahwa belum terdapat satu pun peraturan yang secara eksplisit mengatur izin penggunaan citra dan suara individu dalam format digital yang dihasilkan atau dimanipulasi oleh kecerdasan buatan. Peraturan yang saat ini berlaku, seperti UU PDP, baru mengakomodasi aspek-aspek dasar dari data pribadi dan belum mencakup secara spesifik hak atas citra visual (image rights) maupun mekanisme otentikasi digital terhadap identitas seseorang. Selain itu, peraturan terkait lainnya seperti UU ITE juga belum memberikan definisi atau perlindungan yang memadai terhadap konten digital sintetis yang dapat meniru wajah, suara, atau ekspresi seseorang. Di sisi lain, ketidakhadiran instrumen hukum yang tegas membuat korban penyalahgunaan deepfake tidak memiliki jalur hukum yang jelas dan cepat untuk mendapatkan perlindungan atau pemulihan hak. Masih terbatasnya mekanisme remediasi juga memperkuat indikasi bahwa sistem hukum nasional belum mampu merespons perkembangan teknologi berbasis kecerdasan buatan secara optimal. Untuk memberikan pemetaan awal atas permasalahan tersebut, ditampilkan Tabel 3 yang merangkum dimensi hukum yang beririsan dengan isu deepfake serta status pengaturannya dalam kerangka hukum positif di Indonesia.

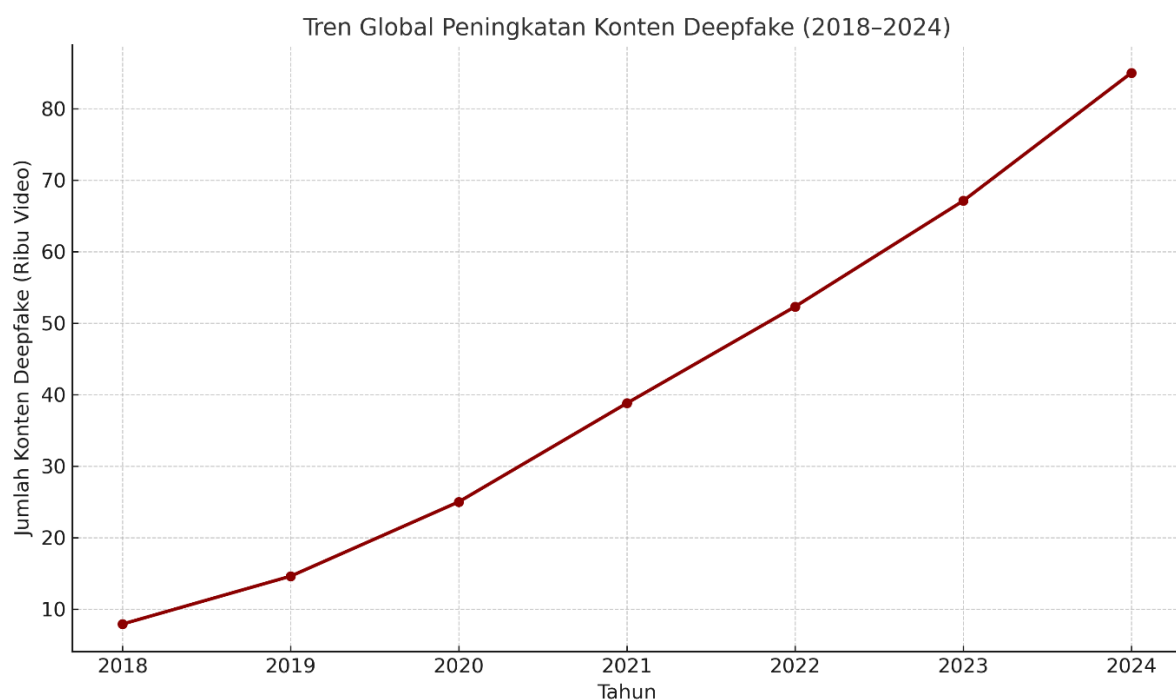
Tabel 1. Dimensi Hukum dan Statusnya dalam Regulasi Indonesia

No	Dimensi Hukum	Status dalam UU PDP/ITE	Keterangan
1	Data Pribadi	Diatur	Fokus pada NIK, nama, alamat, tanpa komponen visual
2	Citra Wajah	Tidak spesifik	Belum dijamin sebagai bagian dari hak identitas
3	Suara Digital	Tidak spesifik	Termasuk konten manipulatif, belum diatur eksplisit
4	Hak atas Otorisasi Digital	Tidak diatur	Tidak ada konsep pengendalian atas citra pribadi
5	Jalur Remediasi Korban	Lemah	Mekanisme pengaduan masih reaktif dan terbatas

Tabel 3 menyajikan lima dimensi hukum yang relevan terhadap keberadaan dan penyalahgunaan teknologi deepfake, serta menilai status pengaturannya dalam UU PDP dan UU ITE. Dimensi pertama, yaitu perlindungan data pribadi, telah diatur dalam UU PDP, namun masih terbatas pada informasi dasar seperti NIK, nama, dan alamat, tanpa mencakup komponen visual seperti citra wajah atau suara digital. Kedua, citra wajah sebagai bagian dari identitas visual seseorang belum dijamin secara spesifik sebagai hak hukum, sehingga membuka potensi penyalahgunaan dalam bentuk representasi visual palsu. Ketiga, suara digital yang dapat dimanipulasi dengan teknologi deepfake juga belum diatur secara eksplisit dalam regulasi yang ada, padahal penggunaannya

semakin meningkat dalam konten yang bersifat menyesatkan atau merugikan. Keempat, hak atas otorisasi digital, yaitu hak individu untuk mengendalikan penggunaan citra dan identitas digitalnya, sama sekali belum memiliki dasar hukum dalam peraturan perundang-undangan Indonesia. Kelima, jalur remediasi bagi korban masih dinilai lemah karena hanya mengandalkan mekanisme pengaduan yang bersifat reaktif dan terbatas dalam cakupan penyelesaiannya. Data dalam tabel ini mengindikasikan bahwa sistem hukum Indonesia masih belum cukup siap dalam menghadapi tantangan hukum dari kemunculan konten digital sintetis, terutama dalam konteks perlindungan identitas digital dan penegakan hak privasi.

Pendekatan yang digunakan dalam penelitian ini adalah yuridis normatif, sehingga tidak dilakukan uji statistik secara kuantitatif terhadap data lapangan. Sebagai gantinya, dilakukan analisis komparatif terhadap muatan norma dalam sejumlah regulasi yang relevan di tingkat nasional dan internasional, dengan fokus pada tiga parameter utama, yaitu perlindungan terhadap konten non-konsensual, cakupan terhadap identitas digital, dan keberadaan sanksi hukum terhadap pelanggaran. Melalui pendekatan ini, dapat diidentifikasi perbedaan tingkat kesiapan hukum dalam menghadapi tantangan dari konten digital berbasis kecerdasan buatan, termasuk teknologi deepfake. Analisis menunjukkan bahwa Uni Eropa telah mengadopsi kerangka hukum yang paling komprehensif melalui GDPR dan AI Act, disusul oleh Inggris dengan Online Safety Act yang secara eksplisit mengatur konten sintetis non-konsensual. Sebaliknya, regulasi di Indonesia belum menunjukkan kemajuan signifikan, baik dalam aspek substantif perlindungan identitas digital maupun mekanisme penegakan hukum yang efektif. Untuk mendukung penjabaran normatif ini, tren peningkatan jumlah konten deepfake secara global juga dianalisis guna menggambarkan urgensi perumusan kebijakan, yang divisualisasikan dalam Gambar 2 berikut.

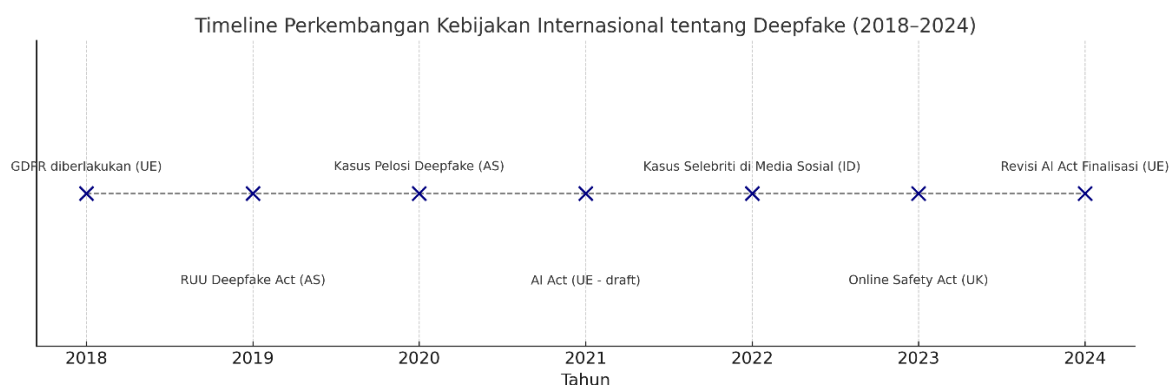


Gambar 2. Grafik Tren Global Peningkatan Konten Deepfake (2018–2024)

Gambar 2 menyajikan data peningkatan jumlah konten deepfake secara global dari tahun 2018 hingga 2024, yang diukur dalam satuan ribu video. Berdasarkan grafik, terlihat adanya kecenderungan naik secara tajam dari sekitar 8 ribu video pada tahun 2018 menjadi lebih dari 85 ribu video pada tahun 2024. Lonjakan ini menunjukkan bahwa produksi konten deepfake mengalami pertumbuhan eksponensial, yang dipengaruhi oleh semakin luasnya akses terhadap

teknologi kecerdasan buatan generatif. Perkembangan algoritma pemrosesan citra dan suara turut mempercepat kemampuan pengguna untuk menghasilkan konten sintetis dengan kualitas tinggi dan tingkat realisme yang sulit dibedakan dari konten asli. Data ini juga mencerminkan meningkatnya potensi risiko penyalahgunaan teknologi tersebut dalam berbagai konteks, termasuk disinformasi, pencemaran nama baik, dan pelanggaran privasi. Visualisasi ini berfungsi untuk memperlihatkan urgensi penyesuaian regulasi digital agar dapat merespons secara tepat terhadap dinamika penyebaran konten deepfake di tingkat global.

Sebagai bagian dari analisis terhadap respons regulatif internasional, penelitian ini juga memetakan perkembangan kebijakan yang berkaitan langsung dengan fenomena deepfake dalam kurun waktu 2018 hingga 2024. Pemetaan ini dilakukan untuk mengidentifikasi korelasi antara dinamika perkembangan teknologi dan munculnya inisiatif regulatif di sejumlah yurisdiksi utama. Beberapa peristiwa yang menjadi titik perhatian meliputi pemberlakuan GDPR oleh Uni Eropa, pengajuan RUU Deepfake Act di Amerika Serikat, serta finalisasi AI Act oleh Uni Eropa pada tahun 2024. Selain itu, kasus-kasus viral seperti video deepfake Nancy Pelosi dan konten selebriti palsu di media sosial turut menjadi pemicu percepatan agenda legislasi. Penyusunan kronologi ini berfungsi sebagai kerangka analisis terhadap arah dan kecepatan respons hukum yang ditunjukkan oleh berbagai negara terhadap ancaman konten non-konsensual berbasis AI. Gambar 3 menyajikan visualisasi linimasa kebijakan internasional yang relevan terhadap isu deepfake selama enam tahun terakhir



Gambar 3. Timeline Perkembangan Kebijakan Internasional tentang Deepfake (2018-2024)

Gambar 3 menampilkan perkembangan kebijakan internasional yang berkaitan dengan isu deepfake dari tahun 2018 hingga 2024 dalam format linimasa horizontal. Setiap titik pada linimasa merepresentasikan baik regulasi yang diimplementasikan maupun insiden penting yang memicu diskursus hukum, seperti pemberlakuan GDPR di Uni Eropa, pengajuan RUU Deepfake Act di Amerika Serikat, dan kemunculan kasus selebriti deepfake di Indonesia. Gambar ini juga mencantumkan proses legislasi penting lain seperti AI Act (draft) oleh Uni Eropa dan Online Safety Act oleh Inggris. Melalui susunan temporal ini, pembaca dapat melihat bahwa kemunculan kasus viral dan meningkatnya tekanan publik sering kali beriringan dengan munculnya inisiatif regulatif baru. Pola ini menunjukkan bahwa respons hukum terhadap teknologi deepfake tidak bersifat seragam, melainkan sangat bergantung pada konteks sosial-politik dan kesiapan institusional di masing-masing negara. Visualisasi ini membantu memperjelas bahwa perkembangan regulasi bersifat dinamis dan terus menyesuaikan diri dengan tingkat kemajuan serta penetrasi teknologi deepfake dalam masyarakat.

D. Hasil Utama yang Signifikan

Temuan utama dari penelitian ini menunjukkan bahwa regulasi hukum di Indonesia masih bersifat umum dan belum responsif terhadap risiko baru yang ditimbulkan oleh konten deepfake.

Ketiadaan norma yang mengatur otorisasi digital dan identitas sintetis telah menciptakan celah hukum yang signifikan dalam perlindungan privasi. Tidak adanya regulasi khusus juga menyebabkan tidak jelasnya tanggung jawab hukum atas platform penyebar konten deepfake seperti media sosial. Selain itu, Indonesia juga belum mengadopsi prinsip-prinsip pengendalian identitas digital sebagaimana diterapkan dalam GDPR atau Online Safety Act yang berlaku di yurisdiksi lain. Situasi ini memperlihatkan bahwa pendekatan regulatif Indonesia belum secara proaktif menyesuaikan diri dengan perkembangan teknologi kecerdasan buatan yang dapat memanipulasi citra dan suara individu. Dalam konteks ini, kebutuhan untuk menyusun kerangka hukum yang mampu memberikan kejelasan terhadap aspek otorisasi digital, akuntabilitas distribusi konten, serta perlindungan identitas digital menjadi semakin relevan seiring meningkatnya ancaman terhadap hak privasi warga negara.

Penelitian ini menunjukkan bahwa sistem hukum di Indonesia belum secara memadai merespons tantangan yang ditimbulkan oleh penyalahgunaan teknologi deepfake, terutama dalam konteks pelanggaran hak privasi. Hasil ini mengonfirmasi bahwa UU PDP dan UU ITE masih berfokus pada perlindungan data dalam pengertian konvensional. Perlindungan yang diberikan belum mencakup aspek-aspek baru seperti citra digital, suara sintetis, atau representasi identitas yang digunakan tanpa persetujuan. Akibatnya, terdapat kekosongan norma hukum yang mengatur hak individu atas otorisasi terhadap representasi digital dirinya. Situasi ini mencerminkan keterbatasan kapasitas hukum nasional dalam menjawab kompleksitas pelanggaran privasi yang ditimbulkan oleh kemajuan teknologi manipulasi digital. Temuan ini juga memberikan dasar awal untuk menjawab pertanyaan utama penelitian mengenai sejauh mana hukum nasional mampu memberikan perlindungan terhadap privasi individu dari konten deepfake.

Temuan penelitian ini selaras dengan argumen yang dikemukakan oleh ²⁹, yang menekankan bahwa deepfake menimbulkan tantangan serius terhadap sistem hukum karena kemampuannya untuk mendistorsi kenyataan dan merusak reputasi secara instan. ³⁰ juga menyatakan bahwa kecepatan distribusi konten deepfake melalui media sosial memperbesar potensi kerusakan yang ditimbulkan terhadap privasi individu. Peneliti seperti ³¹ menambahkan bahwa absennya regulasi yang tegas mengakibatkan dilema etis dalam penggunaan AI untuk manipulasi digital. Penelitian ini memperkuat temuan-temuan tersebut, terutama dalam konteks negara berkembang seperti Indonesia, yang masih tertinggal dalam menyusun regulasi spesifik mengenai konten sintetis. Namun demikian, dibandingkan dengan kerangka hukum di negara-negara seperti Inggris, Amerika Serikat, dan Uni Eropa, posisi Indonesia masih jauh tertinggal. Sebagai contoh, Online Safety Act di Inggris telah menetapkan larangan distribusi konten deepfake tanpa persetujuan dan memberikan sanksi hukum yang tegas terhadap pelanggar. Hal serupa ditemukan dalam AI Act dan GDPR di Uni Eropa, yang tidak hanya menetapkan batasan hukum tetapi juga memberikan hak otorisasi atas data biometrik dan citra digital. Di sisi lain, UU PDP Indonesia belum memuat norma mengenai citra wajah atau suara sebagai bagian dari data pribadi sensitif, seperti dikemukakan oleh ³².

Salah satu temuan yang menarik adalah tidak adanya definisi hukum mengenai “identitas digital” dalam peraturan perundang-undangan Indonesia, meskipun konsep ini menjadi inti dari berbagai regulasi internasional mengenai teknologi AI. Konsep identitas digital mencakup berbagai elemen seperti citra wajah, ekspresi suara, dan gerakan tubuh yang kini telah menjadi komponen utama dalam proses rekayasa konten deepfake, sehingga keberadaannya dalam kerangka hukum menjadi sangat penting. Ketidakhadiran konsep ini dalam sistem hukum nasional menimbulkan celah regulatif yang menyulitkan dalam perlindungan hak-hak individu di

²⁹ Ghiurău and Popescu.

³⁰ Islam and others.

³¹ Dhirani and others.

³² Ferrari.

ranah digital. Selain itu, hasil penelitian menunjukkan bahwa mekanisme remediasi terhadap korban deepfake di Indonesia belum tersedia dalam bentuk yang operasional dan mudah diakses oleh masyarakat. Peneliti sebelumnya seperti ³³ menekankan pentingnya kejelasan jalur remediasi hukum dalam membangun kepercayaan publik terhadap sistem hukum digital, yang berarti bahwa keberadaan saluran pemulihan hukum yang jelas akan mendorong rasa aman dalam penggunaan teknologi. Namun, temuan ini menunjukkan bahwa sistem hukum Indonesia masih bersifat reaktif dan fragmentaris dalam merespons pelanggaran hak digital, sehingga diperlukan pembaruan kebijakan hukum yang dapat mengakomodasi dinamika baru yang dihadirkan oleh perkembangan teknologi kecerdasan buatan.

Secara teoritis, penelitian ini memperluas cakupan kajian hukum digital dengan memperkenalkan dimensi otorisasi citra dan suara sebagai bagian integral dari hak privasi individu dalam ruang digital. Konsep ini memperkaya pendekatan privasi kontekstual yang dikemukakan oleh ³⁴, yang menekankan pentingnya mempertimbangkan konteks sosial dan teknologi dalam pengaturan data pribadi. Selain itu, relevansi prinsip tanggung jawab etis dalam desain sistem kecerdasan buatan yang disarankan oleh ³⁵ semakin mengemuka ketika dikaitkan dengan kebutuhan perlindungan terhadap penyalahgunaan citra digital. Di sisi praktis, temuan ini menyoroti urgensi reformulasi regulasi nasional agar mampu menjawab tantangan yang dihadirkan oleh konten digital berbasis kecerdasan buatan, yang terus berkembang secara dinamis. Reformulasi ini mencakup penyusunan definisi hukum yang komprehensif mengenai konten sintesis, pengakuan identitas digital sebagai hak hukum yang dilindungi, serta penetapan sanksi hukum terhadap pelanggaran privasi melalui penyebaran konten deepfake non-konsensual. Implikasi yang dihasilkan dari temuan ini berkontribusi tidak hanya dalam ranah akademik dan regulatif, tetapi juga berdampak langsung pada praktik di sektor teknologi informasi, penyelenggara platform digital, serta aparat penegak hukum yang bertanggung jawab dalam menangani pelanggaran di ruang siber.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan untuk menempatkan hasil temuan dalam konteks yang tepat. Pertama, pendekatan normatif yang digunakan cenderung membatasi eksplorasi terhadap pengalaman langsung para korban maupun aparat penegak hukum dalam menghadapi kasus-kasus pelanggaran berbasis teknologi deepfake. Keterbatasan ini mengurangi kedalaman pemahaman terhadap realitas sosial dan tantangan teknis dalam penerapan hukum di lapangan. Kedua, penelitian belum secara empiris mengkaji efektivitas regulasi yang ada dalam praktik peradilan atau kebijakan publik, sehingga belum dapat memberikan gambaran utuh mengenai implementasi dan kendala pelaksanaannya. Ketiga, cakupan perbandingan hukum yang dilakukan dalam studi ini masih terbatas pada yurisdiksi yang sudah sering dibahas dalam literatur internasional, seperti Inggris dan Uni Eropa, dan belum menyertakan negara-negara berkembang lain yang memiliki karakteristik hukum serupa dengan Indonesia. Selain itu, keterbatasan metodologis ini juga berdampak pada potensi generalisasi temuan yang mungkin tidak sepenuhnya mencerminkan variasi kondisi sosial, politik, dan teknologi antarnegara. Oleh karena itu, penting untuk memahami hasil studi ini sebagai langkah awal yang masih memerlukan verifikasi dan elaborasi lebih lanjut melalui pendekatan yang lebih holistik.

Berdasarkan berbagai keterbatasan yang telah diidentifikasi, penelitian selanjutnya disarankan untuk mengintegrasikan pendekatan normatif dan empiris guna memperoleh pemahaman yang lebih komprehensif. Penggabungan metode ini dapat dilakukan melalui wawancara mendalam dengan praktisi hukum, regulator, korban pelanggaran privasi digital, serta perwakilan dari platform teknologi, guna menjaring perspektif yang lebih beragam dan kontekstual. Penelitian

³³ Mania.

³⁴ Matli.

³⁵ Dhirani and others.

mendatang juga memiliki potensi untuk mengembangkan konsep “hak atas identitas digital” sebagai kerangka teoritis baru dalam hukum siber Indonesia, yang belum banyak dieksplorasi secara sistematis. Selain itu, perhatian lebih besar perlu diberikan pada studi mengenai tanggung jawab hukum penyedia platform digital, khususnya dalam hal mekanisme penyaringan dan penanganan konten deepfake yang bersifat merugikan. Kajian ini diharapkan dapat memperkuat landasan regulatif dalam upaya menciptakan ruang digital yang lebih aman dan akuntabel. Penelitian komparatif dengan negara-negara di Asia Tenggara yang menghadapi tantangan serupa juga dapat memberikan kontribusi berharga dalam merumuskan kerangka kerja regulatif berbasis kolaborasi regional, misalnya melalui pengembangan standar ASEAN-level untuk penanganan konten sintetis dan perlindungan identitas digital.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa fenomena deepfake membawa ancaman serius terhadap hak privasi dan integritas identitas digital individu, khususnya dalam konteks belum adanya perlindungan hukum yang memadai di Indonesia. Ketidakhadiran norma hukum yang secara eksplisit mengatur otorisasi citra dan suara digital mengindikasikan celah regulatif yang signifikan dalam sistem hukum nasional. Meskipun Indonesia telah memiliki UU PDP dan UU ITE, kedua undang-undang ini belum mencakup aspek representasi digital yang dihasilkan atau dimanipulasi oleh kecerdasan buatan. Hal ini berbeda dengan pendekatan di yurisdiksi lain seperti Inggris dan Uni Eropa, yang telah memiliki instrumen hukum progresif seperti Online Safety Act dan GDPR. Fakta ini memperlihatkan bahwa sistem hukum Indonesia masih bersifat reaktif dan kurang adaptif terhadap tantangan teknologi digital yang berkembang pesat. Oleh karena itu, diperlukan langkah konkret dalam merumuskan kebijakan hukum yang mampu melindungi hak-hak digital warga negara secara komprehensif.

Penelitian selanjutnya disarankan untuk mengintegrasikan pendekatan normatif dengan metode empiris guna memperoleh gambaran yang lebih komprehensif mengenai dampak dan respons terhadap penyalahgunaan konten deepfake. Penggalan data melalui wawancara dengan praktisi hukum, regulator, dan korban akan memberikan perspektif yang lebih mendalam tentang tantangan penegakan hukum di lapangan. Selain itu, penting untuk mengembangkan kerangka hukum mengenai “hak atas identitas digital” yang belum diatur dalam sistem hukum Indonesia saat ini. Studi komparatif lintas negara berkembang di kawasan Asia Tenggara juga perlu diperluas guna merumuskan standar regional penanganan konten sintetis. Penelitian mendatang diharapkan mampu merumuskan model regulasi berbasis prinsip keadilan digital dan akuntabilitas teknologi, yang dapat diterapkan dalam konteks lokal Indonesia. Dengan demikian, kontribusi akademik dari penelitian-penelitian berikutnya dapat memperkuat landasan hukum nasional dalam menghadapi risiko etis dan hukum akibat perkembangan teknologi kecerdasan buatan.

DAFTAR PUSTAKA

- Aseeva, Anna, ‘Liable and Sustainable by Design: A Toolbox for a Regulatory Compliant and Sustainable Tech’, *Sustainability*, 16.1 (2023), p. 228, doi:10.3390/su16010228
- Asimakopoulou, George, Hera Antonopoulou, Konstantinos Giotopoulos, and Constantinos Halkiopoulos, ‘Impact of Information and Communication Technologies on Democratic Processes and Citizen Participation’, *Societies*, 15.2 (2025), p. 40, doi:10.3390/soc15020040
- Axelsson, Kaya, Claire Wigg, and Matilda Becker, ‘Is Impact Out of Scope? A Call for Innovation in Climate Standards to Inspire Action Across Companies’ Spheres of Influence’, *Carbon Management*, 15.1 (2024), p. 2382995, doi:10.1080/17583004.2024.2382995

Bakiner, Onur, 'The Promises and Challenges of Addressing Artificial Intelligence with Human Rights', *Big Data and Society*, 10.2 (2023), pp. 1–13, doi:10.1177/20539517231205476

Clare, McGlynn, and Rüya Tuna Toparlak, 'The "New Voyeurism": Criminalizing the Creation of "Deepfake Porn"', *Journal of Law and Society*, 52.2 (2025), pp. 204–28, doi:10.1111/jols.12527

Dhirani, Lubna Luxmi, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe, 'Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review', *Sensors*, 23.3 (2023), p. 1151, doi:10.3390/s23031151

Falcone, Pasquale Marcello, 'Sustainable Energy Policies in Developing Countries: A Review of Challenges and Opportunities', *Energies*, 16.18 (2023), p. 6682, doi:10.3390/en16186682

Ferrari, Ms Valeria, 'The Platformisation of Digital Payments: The Fabrication of Consumer Interest in the EU FinTech Agenda', *Computer Law & Security Review*, 45 (2022), p. 105687, doi:10.1016/j.clsr.2022.105687

Ghiurău, David, and Daniela Elena Popescu, 'Distinguishing Reality from AI: Approaches for Detecting Synthetic Content', *Computers*, 14.1 (2024), p. 1, doi:10.3390/computers14010001

Hossain, Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, and Yue Xu, 'Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework', *Applied Sciences*, 14.13 (2024), p. 5501, doi:10.3390/app14135501

Islam, Masabah Bint E., Muhammad Haseeb, Hina Batool, Nasir Ahtasham, and Zia Muhammad, 'AI Threats to Politics, Elections, and Democracy: A Blockchain-Based Deepfake Authenticity Verification Framework', *Blockchains*, 2.4 (2024), pp. 458–81, doi:10.3390/blockchains2040020

Jørgensen, Bo Nørregaard, and Zheng Grace Ma, 'Regulating AI in the Energy Sector: A Scoping Review of EU Laws, Challenges, and Global Perspectives', *Energies*, 18.9 (2025), p. 2359, doi:10.3390/en18092359

Kira, Beatriz, 'When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act', *Computer Law & Security Review*, 54 (2024), p. 106024, doi:10.1016/j.clsr.2024.106024

Kirschschlaeger, Peter G., 'An International Data-Based Systems Agency IDA: Striving for a Peaceful, Sustainable, and Human Rights-Based Future', *Philosophies*, 9.3 (2024), pp. 1–22, doi:10.3390/philosophies9030073

Labs, Deeptrace, *The State of Deepfakes: Landscape, Threats, and Impact*, 2019 <<https://www.deeptracelabs.com/resources>>

Mania, Karolina, 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study', *Trauma, Violence, and Abuse*, 25.1 (2024), pp. 117–29, doi:10.1177/15248380221143772

Matli, Walter, 'Extending the Theory of Information Poverty to Deepfake Technology', *International Journal of Information Management Data Insights*, 4.2 (2024), p. 100286, doi:10.1016/j.jjime.2024.100286

Morley, Bruce, and Ionel Bostan, 'Consolidating the Role of AI in the Economy and Society: Combating the Deepfake Phenomenon Through Strategic and Normative Approaches—The Case of Romania in the EU Context', *Economies*, 13.5 (2025), p. 129, doi:10.3390/economies13050129

Mustak, Mekhail, Joni Salminen, Matti Mäntymäki, Arafat Rahman, and Yogesh K. Dwivedi,

‘Deepfakes: Deceptions, Mitigations, and Opportunities’, *Journal of Business Research*, 154 (2023), p. 113368, doi:10.1016/j.jbusres.2022.113368

Naffi, Nadia, Mélodie Charest, Sarah Danis, Laurie Pique, Ann Louise Davidson, Nicolas Brault, and others, ‘Empowering Youth to Combat Malicious Deepfakes and Disinformation: An Experiential and Reflective Learning Experience Informed by Personal Construct Theory’, *Journal of Constructivist Psychology*, 38.1 (2023), pp. 119–40, doi:10.1080/10720537.2023.2294314

Observatory, Stanford Internet, *SIO 2022 Annual Report*, 2022 <https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2023-01/sio2022_annual_report_v5.pdf>

Parti, Katalin, and Judit Szabó, ‘The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe’, *Laws*, 13.6 (2024), p. 67, doi:10.3390/laws13060067

Pawelec, Maria, and Maria Mariapawelec, ‘Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions’, *Digital Society*, 1.2 (2022), pp. 1–37, doi:10.1007/s44206-022-00010-6

Pedersen, Kristoffer Torngaard, Lauritz Pepke, Tobias Staermose, Maria Papaioannou, Gaurav Choudhary, and Nicola Dragoni, ‘Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments’, *Journal of Cybersecurity and Privacy*, 5.2 (2025), p. 18, doi:10.3390/jcp5020018

Raghav, Manjula, and Sanjana Sharma Marwaha, ‘Challenges and Issues in India’s Legal Framework for the Right to Privacy in Cyberspace’, *Fiat Justisia: Jurnal Ilmu Hukum*, 17.1 (2023), pp. 1–16, doi:10.25041/fiatjustisia.v17no1.2667

Romero Moreno, Felipe, ‘Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content’, *International Review of Law, Computers and Technology*, 38.3 (2024), pp. 297–326, doi:10.1080/13600869.2024.2324540

Van der Sloot, Bart, and Yvette Wagenveld, ‘Deepfakes: Regulatory Challenges for the Synthetic Society’, *Computer Law & Security Review*, 46 (2022), p. 105716, doi:10.1016/j.clsr.2022.105716

Sunvy, Ahmed Shafkat, Raiyan Bin Reza, and Abdullah Al Imran, ‘Media Coverage of DeepFake Disinformation: An Analysis of Three South-Asian Countries’, *Informasi*, 53.2 (2023), pp. 295–308, doi:10.21831/informasi.v53i2.66479