Rekonstruksi *Obstruction of Justice* atas Manipulasi *Adversarial* Bukti Elektronik Berbasis *AI* dalam KUHP dan KUHAP Indonesia

Andre Kurniawan[1*], Herlita Eryke[2]
[1*,2]Program Studi Magister Hukum, Fakultas Hukum, Universitas Bengkulu
Corresponding Author's e-mail : andrekurniawan552001@gmail.com

SEIKAT
Jurnal Ilmu Sosial, Politik dan Hukum

e-ISSN: 2964-0962

SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum

https://ejournal.45mataram.ac.id/index.php/seikat

Vol. 5, No. 5, Oktober 2026

Page: 3575 - 3590

Available at:

https://ejournal.45mataram.ac.id/index.php/seikat/article/view/4426

DOI:

https://doi.org/10.55681/seikat.v5i5.4426

Article History:

Received: 22-09-2026
Revised: 13-10-2026
Accepted: 14-10-2026

Abstract *: The development of artificial intelligence has transformed criminal evidence, particularly when electronic evidence is not merely falsified but adversarially manipulated to deceive AI-based analytical systems. This study aims to reconstruct the concept of obstruction of justice concerning adversarial manipulation of electronic evidence within Indonesia's Criminal Code and Criminal Procedure Code. It employs normative legal research using statutory, conceptual, case, and comparative approaches. The findings show that adversarial manipulation differs from conventional digital falsification because attacks may target an AI system's inference process without significantly altering the visible appearance of evidence. Normatively, Article 278 of the Criminal Code has the strongest connection to direct manipulation of evidence, while Articles 281 and 282 may only apply when their specific elements are satisfied. In procedural law, electronic evidence authentication should be supplemented by assessment of analytical reliability, including model transparency, error rates, reproducibility, and adversarial robustness. This study proposes the Adversarial Evidence Interference Test, consisting of judicial-process nexus, adversarial act, knowledge and purpose, material interference capability, and forensic causal traceability. This reconstruction enables criminal law to adapt to AI developments without expanding criminalization by analogy and strengthens protection for the integrity of criminal evidentiary processes. It promotes accountable, transparent, and reviewable digital adjudication.*

Keywords: *Obstruction of justice; Adversarial manipulation; Electronic evidence; Artificial intelligence; Criminal evidence.*

Abstrak : Perkembangan *artificial intelligence* telah mengubah karakter pembuktian pidana, khususnya ketika bukti elektronik tidak hanya dipalsukan, tetapi dimanipulasi secara adversarial untuk mengecoh sistem analitik berbasis AI. Penelitian ini bertujuan merekonstruksi konsep *obstruction of justice* terhadap manipulasi adversarial bukti elektronik dalam kerangka KUHP dan KUHAP Indonesia. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan. Hasil penelitian menunjukkan bahwa manipulasi adversarial memiliki karakter berbeda dari pemalsuan digital konvensional karena serangan dapat diarahkan pada proses inferensi sistem AI tanpa mengubah tampilan bukti secara signifikan. Secara normatif, Pasal 278 KUHP memiliki kedekatan paling kuat terhadap manipulasi langsung atas alat bukti, sedangkan Pasal 281 dan Pasal 282 hanya dapat diterapkan apabila unsur khusus masing-masing terpenuhi. Dalam hukum acara, autentisitas bukti elektronik perlu dilengkapi dengan pengujian reliabilitas proses analitik, termasuk transparansi model, tingkat kesalahan, reproduktibilitas, dan *adversarial robustness*. Penelitian ini menawarkan *Adversarial Evidence Interference Test* sebagai parameter yang mencakup *judicial-process nexus, adversarial act, knowledge and purpose, material interference capability*, serta *forensic causal traceability*. Rekonstruksi tersebut menjaga adaptivitas hukum pidana terhadap perkembangan AI tanpa memperluas kriminalisasi melalui analogi serta memperkuat perlindungan

terhadap integritas proses pembuktian pidana. Model tersebut menyediakan dasar konseptual bagi standar pembuktian digital yang akuntabel, transparan, konsisten, serta berorientasi pada *due process*.

Kata kunci: O*bstruction of justice*; Manipulasi adversarial; Bukti elektronik; A*rtificial intelligence*; Pembuktian pidana.

PENDAHULUAN

Perkembangan kecerdasan buatan telah mengubah karakter pembuktian pidana dari model yang bertumpu pada objek fisik dan informasi elektronik konvensional menuju pembuktian yang semakin bergantung pada proses komputasional. Perubahan tersebut tidak hanya terlihat dari munculnya gambar, rekaman suara, video, dan dokumen sintetis, tetapi juga dari penggunaan AI untuk mengidentifikasi pola, memverifikasi autentisitas, serta membantu analisis terhadap bukti digital. Konsekuensinya, persoalan hukum pembuktian tidak lagi berhenti pada pertanyaan apakah suatu file elektronik asli atau palsu. Persoalan bergeser pada apakah metode komputasional yang menghasilkan, memproses, atau menilai bukti tersebut dapat dipercaya. Kajian mutakhir mengenai sistem peradilan Indonesia bahkan menunjukkan bahwa penggunaan AI menimbulkan persoalan baru menyangkut reliabilitas bukti digital, akuntabilitas algoritma, bias data, dan independensi penilaian hakim. Pada saat yang sama, penelitian mengenai bukti elektronik Indonesia menunjukkan bahwa perkembangan regulasi belum sepenuhnya diikuti tata kelola digital evidence yang koheren.[1]

Ancaman yang lebih kompleks muncul ketika kelemahan sistem AI tidak sekadar digunakan untuk menghasilkan bukti palsu melalui *deepfake*, tetapi sengaja dieksploitasi agar sistem AI memberikan kesimpulan yang keliru terhadap suatu bukti. Fenomena tersebut berkaitan dengan *adversarial machine learning*, yakni manipulasi yang dirancang untuk memengaruhi perilaku atau keluaran model pembelajaran mesin. National Institute of Standards and Technology mengklasifikasikan berbagai bentuk serangan tersebut, antara lain *evasion*, *poisoning*, dan bentuk penyalahgunaan lain terhadap sistem AI. Dalam konteks pembuktian, *evasion attack* dapat bekerja dengan menambahkan perubahan yang secara kasatmata hampir tidak terlihat pada gambar, suara, atau video, tetapi cukup untuk mengubah klasifikasi sistem AI. Penelitian eksperimental menunjukkan bahwa *deepfake detector* memang dapat dikelabui melalui *adversarial perturbations*. Dengan demikian, bukti palsu secara teoritis dapat direkayasa agar lolos sebagai autentik, sementara bukti autentik dapat dimodifikasi agar sistem menilainya sebagai tidak terpercaya.[2]

Persoalan tersebut mempunyai konsekuensi hukum yang berbeda dari kejahatan *deepfake* konvensional. Dalam *deepfake* biasa, titik perhatian hukum umumnya berada pada pembuatan atau penggunaan konten sintetis. Pada manipulasi adversarial, sasaran serangan dapat bergeser kepada mekanisme epistemik proses peradilan, yaitu perangkat atau metode yang digunakan penyidik, ahli, penuntut umum, dan hakim untuk membedakan bukti autentik dari bukti yang telah direkayasa. Kajian sistematis mengenai *deepfake* dalam sistem peradilan pidana telah mengidentifikasi pemalsuan dan modifikasi bukti, persoalan atribusi, serta erosi kepercayaan terhadap bukti audio-visual sebagai ancaman serius. Penelitian lain bahkan menunjukkan perlunya menilai bukan hanya hasil suatu *deepfake detector*, melainkan validitas model, tingkat kesalahan, ketahanan terhadap serangan, kemampuan generalisasi, keterlacakan, dan reproduktibilitas proses analisisnya. Persoalan tersebut memperlihatkan bahwa serangan

[1] Jamil, A., & Saifuddin, S. (2026). The use of artificial intelligence in the court process in Indonesia. Lex Scientia Law Review, 10(1), 521–550. https://doi.org/10.15294/lslr.v10i1.28681; Sumardiana, B., et al. (2024). Evaluation of electronic evidence in criminal justice. Indonesian Journal of Criminal Law Studies, 9(2), 309–332. https://doi.org/10.15294/ijcls.v9i2.36634.

[2] Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2024). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2e2023). https://doi.org/10.6028/NIST.AI.100-2e2023; Chen, P., Xu, M., & Qi, J. (2024). DeepFake detection against adversarial examples based on D-VAEGAN. IET Image Processing, 18(3), 615–626. https://doi.org/10.1049/ipr2.12973.

terhadap AI forensik dapat mengganggu pencarian kebenaran materiil meskipun pelaku tidak menghapus bukti secara fisik.[3]

Urgensi persoalan semakin meningkat setelah Indonesia memasuki rezim hukum acara pidana baru. Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana berlaku sejak 2 Januari 2026. Pasal 235 ayat (1) huruf f secara tegas mengakui bukti elektronik sebagai alat bukti, sedangkan huruf e mengatur barang bukti dan huruf h membuka kategori alat bukti lain sepanjang diperoleh secara tidak melawan hukum. Pasal 235 ayat (3) mensyaratkan agar autentikasi alat bukti dapat dibuktikan dan perolehannya sah; ayat (4) memberi hakim kewenangan menilai kedua aspek tersebut; dan ayat (5) meniadakan penggunaan dan kekuatan pembuktian alat bukti yang tidak autentik dan/atau diperoleh secara melawan hukum. Namun, ketentuan ini belum merumuskan protokol khusus untuk memeriksa keandalan model AI ketika model tersebut menjadi sasaran manipulasi adversarial.[4]

Persoalan berikutnya berada pada hukum pidana materiil. Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, yang berlaku sejak 2 Januari 2026, mengatur tindak pidana terhadap proses peradilan dalam Bab VI Buku Kedua. Pasal 278 ayat (1) huruf a meliputi tindakan memalsukan, membuat, atau mengajukan bukti palsu; huruf c meliputi tindakan mengubah, merusak, menyembunyikan, menghilangkan, atau menghancurkan alat bukti. Pasal 281 mengatur tindakan yang ditujukan kepada pejabat penyidikan, penuntutan, pemeriksaan persidangan, atau pelaksanaan putusan dengan maksud khusus memaksa atau membujuk pejabat melakukan atau tidak melakukan tugasnya. Pasal 282 ayat (1) huruf a dan b mengatur penyembunyian orang yang melakukan tindak pidana atau pemberian pertolongan agar orang tersebut melarikan diri dari proses hukum. Ketiganya mempunyai unsur perbuatan serta sasaran berbeda, sehingga tidak boleh dipertukarkan hanya karena sama-sama berkaitan dengan proses peradilan.[5]

Konfigurasi norma tersebut memunculkan persoalan ketika modus yang digunakan pelaku tidak berbentuk penghancuran file, penghilangan barang bukti, intimidasi terhadap penyidik, ataupun penyembunyian tersangka, melainkan manipulasi terhadap data atau input dengan tujuan mengecoh sistem AI yang digunakan dalam pemeriksaan forensik. Sebagai contoh, pelaku dapat mempertahankan keberadaan rekaman elektronik tetapi menambahkan *adversarial perturbation* agar sistem deteksi memberikan *false negative*. Dalam situasi lain, manipulasi dapat diarahkan untuk membuat rekaman autentik menghasilkan *false positive* sehingga dipersepsikan sebagai hasil rekayasa. Secara fungsional, kedua tindakan tersebut dapat merusak proses penemuan fakta. Namun, secara dogmatis muncul pertanyaan apakah perbuatan tersebut merupakan "mengubah" alat bukti dalam Pasal 278, tindakan "menghalang-halangi atau memengaruhi pejabat" dalam Pasal 281, bentuk tindak pidana siber tersendiri, atau gabungan beberapa delik. Ketidakjelasan kualifikasi inilah yang membedakan persoalan manipulasi adversarial dari pembahasan *deepfake* sebagai kejahatan siber pada umumnya.[6]

Konstruksi terhadap modus baru tersebut tidak dapat dilakukan hanya dengan memperluas arti *obstruction of justice* secara bebas. Hukum pidana terikat pada asas legalitas yang menuntut rumusan delik dapat diprediksi dan tidak dikembangkan melalui analogi yang merugikan terdakwa. Persoalan menjadi semakin penting setelah Mahkamah Konstitusi dalam

[3] Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. Crime Science, 13, Article 41. https://doi.org/10.1186/s40163-024-00239-1; Azis, M. A., Pujiyono, & Putri, R. A. K. (2026). Reconstructing reliability standards for deepfake detectors. West Science Law and Human Rights, 4(3), 299–309. https://doi.org/10.58812/wslhr.v4i03.3022.

[4] Republik Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, Pasal 235 ayat (1) huruf e, f, dan h serta ayat (3)–(5). https://peraturan.go.id/id/uu-no-20-tahun-2025.

[5] Republik Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Pasal 278 ayat (1) huruf a dan c, Pasal 281, dan Pasal 282 ayat (1) huruf a–b. https://www.peraturan.go.id/files/uu1-2023.pdf; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice" dalam pengaturan Undang-Undang Nomor 1 Tahun 2023. https://doi.org/10.61994/jsls.v2i2.651.

[6] Republik Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023, Pasal 278 ayat (1) huruf a dan c serta Pasal 281–282. https://www.peraturan.go.id/files/uu1-2023.pdf; Vassilev, A., et al. (2024). Adversarial machine learning. https://doi.org/10.6028/NIST.AI.100-2e2023.

Putusan Nomor 71/PUU-XXIII/2025 tanggal 2 Maret 2026 menyatakan frasa "secara langsung atau tidak langsung" dalam Pasal 21 Undang-Undang Pemberantasan Tindak Pidana Korupsi bertentangan dengan UUD 1945 dan tidak mempunyai kekuatan hukum mengikat. Mahkamah menilai frasa tersebut berpotensi memiliki sifat lentur sehingga dapat menjangkau pihak yang dianggap menghalangi proses hukum tanpa batas yang memadai. Meskipun putusan tersebut menguji norma UU Tipikor dan bukan Pasal 278 atau Pasal 281 KUHP, pertimbangannya relevan secara konseptual dalam menunjukkan bahwa adaptasi delik *obstruction of justice* terhadap teknologi baru harus tetap tunduk pada kepastian rumusan, hubungan kausal, serta pembuktian maksud pelaku.[7]

Pada sisi hukum pembuktian, persoalannya tidak kalah serius. Pengakuan formal terhadap bukti elektronik belum otomatis menjamin reliabilitas hasil pemeriksaannya. Penelitian tahun 2026 mengenai kerangka bukti elektronik Indonesia menemukan bahwa persoalan pengumpulan, autentikasi, penanganan, preservasi, dan evaluasi bukti digital masih memerlukan arsitektur tata kelola yang lebih terstruktur. Penelitian komparatif mengenai penggunaan AI sebagai bukti elektronik juga menunjukkan bahwa persoalan yang berkembang telah bergeser dari pertanyaan tentang dapat atau tidaknya bukti elektronik diterima menuju standar untuk menilai autentisitas, integritas, keterlacakan proses, kinerja model, verifikasi, dan akuntabilitas sistem AI. Kondisi tersebut menjadi semakin problematik ketika serangan adversarial dapat dirancang justru untuk mengeksploitasi parameter teknis yang menentukan reliabilitas hasil pemeriksaan. Dengan demikian, Pasal 235 KUHAP menghadapi problem bukan hanya mengenai autentikasi bukti, tetapi juga mengenai autentikasi dan reliabilitas proses yang digunakan untuk mengautentikasi bukti.[8]

Pemetaan penelitian terdahulu memperlihatkan ruang ilmiah yang masih terbuka. Sumardiana et al. (2024) mengulas kedudukan bukti elektronik pada era AI, sedangkan Antoro et al. (2026) membahas penerimaan AI sebagai bukti elektronik melalui pendekatan komparatif. Azis et al. (2026) merekonstruksi standar reliabilitas *deepfake detector*, meliputi validitas model, tingkat kesalahan, ketahanan, keterlacakan, dan akuntabilitas. Sandoval et al. (2024) mengulas secara sistematis ancaman deepfake terhadap pembuktian pidana; Capra (2024) mengkaji persoalan autentikasi deepfake menurut hukum pembuktian Amerika Serikat. Secara teknis, Chen et al. (2024), Hooda et al. (2024), dan Cirillo et al. (2025) menunjukkan atau menguji kerentanan pendeteksi deepfake terhadap serangan adversarial dengan lingkup eksperimen yang berbeda. Adapun Pettanasse et al. (2024) membahas delik perintangan proses peradilan berdasarkan KUHP Nasional. Literatur tersebut belum secara langsung menghubungkan serangan pada proses inferensi AI dengan pembuktian unsur setiap delik dalam Pasal 278, 281, dan 282 KUHP.[9]

Berdasarkan peta penelitian itu, celah kajian terdapat pada persilangan antara hukum pembuktian berbasis AI dan delik terhadap proses peradilan. Penelitian tentang deepfake dan digital forensik menekankan autentikasi, validasi, reliabilitas, serta risiko salah klasifikasi (Sandoval et al., 2024; Azis et al., 2026; Capra, 2024). Sebaliknya, kajian pidana nasional menempatkan perhatian pada batas unsur perbuatan, objek perlindungan, dan kesengajaan dalam tindak pidana terhadap proses peradilan (Pettanasse et al., 2024). Belum memadai kajian

[7] Mahkamah Konstitusi Republik Indonesia. (2026c). Putusan Nomor 71/PUU-XXIII/2025 (2 Maret 2026), pengujian Pasal 21 UU Tipikor. https://www.mkri.id/berita/mk-hapus-pasal-karet-%E2%80%9Cobstruction-of-justice%E2%80%9D-24696.

[8] Antoro, H., Budhijanto, D., & Somawijaya. (2026). Admissibility of artificial intelligence as electronic evidence. Jurnal IUS Kajian Hukum dan Keadilan, 14(1), 122–139. https://doi.org/10.29303/ius.v14i1.1880; Agatha, C., & Rahaditya, R. (2026). Fragmented digital forensic standards in Indonesian criminal evidence. https://doi.org/10.21070/ijler.v21i2.1558; Republik Indonesia. (2025). UU No. 20 Tahun 2025, Pasal 235.

[9] Pemetaan pustaka: Sumardiana et al. (2024), https://doi.org/10.15294/ijcls.v9i2.36634; Antoro et al. (2026), https://doi.org/10.29303/ius.v14i1.1880; Azis et al. (2026), https://doi.org/10.58812/wslhr.v4i03.3022; Sandoval et al. (2024), https://doi.org/10.1186/s40163-024-00239-1; Capra (2024), https://ir.lawnet.fordham.edu/flr/vol92/iss6/7/; Chen et al. (2024), https://doi.org/10.1049/ipr2.12973; Hooda et al. (2024), https://doi.org/10.1109/WACV57701.2024.00377; Cirillo et al. (2025), https://doi.org/10.1186/s13635-025-00211-9; Pettanasse et al. (2024), https://doi.org/10.61994/jsls.v2i2.651. Detail lengkap tercantum dalam daftar pustaka.

yang secara terpadu menguji apakah intervensi komputasional yang mengubah keluaran model, tetapi tidak selalu mengubah tampilan bukti bagi manusia, dapat memenuhi rumusan delik yang berlaku tanpa analogi yang merugikan terdakwa.[10]

Kebaruan penelitian ini terletak pada rekonstruksi normatif manipulasi adversarial sebagai dugaan intervensi terhadap proses peradilan, bukan pada pembahasan umum *deepfake* atau bukti elektronik. Analisis memisahkan perubahan alat bukti menurut Pasal 278 KUHP, tindakan terhadap pejabat dengan maksud khusus menurut Pasal 281, bantuan kepada pelaku menurut Pasal 282, serta autentikasi dan legalitas perolehan alat bukti menurut Pasal 235 KUHAP. Rekonstruksi juga menuntut pembuktian kesengajaan, hubungan dengan proses peradilan, materialitas pengaruh, dan keterlacakan kausalitas forensik. Kerangka tersebut ditempatkan sebagai alat analisis, bukan penciptaan unsur tindak pidana baru.[11]

Atas dasar itu, penelitian tentang *"Rekonstruksi Obstruction of Justice* atas Manipulasi Adversarial Bukti Elektronik Berbasis AI dalam KUHP dan KUHAP Indonesia" menjawab tiga pertanyaan: (1) bagaimana karakter manipulasi adversarial atas bukti elektronik dibedakan dari pemalsuan digital biasa; (2) sampai di mana Pasal 278, 281, dan 282 KUHP dapat diterapkan dengan tetap menghormati asas legalitas; dan (3) bagaimana standar autentikasi serta pembuktian kausalitas menurut Pasal 235 KUHAP dapat direkonstruksi ketika hasil analisis AI digunakan dalam pembuktian pidana? Ketiga pertanyaan dijawab melalui pendekatan normatif-doktrinal dengan pembanding teknis dan regulasi internasional, tanpa mengklaim telah memvalidasi AEIT secara empiris.

METODE PENELITIAN

Penelitian ini menggunakan penelitian hukum normatif atau doktrinal dengan karakter preskriptif-analitis. Pilihan tersebut didasarkan pada objek penelitian yang tidak mengukur perilaku penggunaan artificial intelligence secara empiris, melainkan menguji kecukupan struktur norma hukum pidana dalam mengkualifikasikan *adversarial manipulation* terhadap bukti elektronik sebagai perbuatan yang mengganggu proses peradilan. Penelitian normatif memungkinkan peneliti mengidentifikasi ketidakjelasan norma, membangun hubungan antarketentuan, menilai konsistensi doktrin, serta merumuskan konstruksi hukum terhadap persoalan yang belum memperoleh pengaturan secara eksplisit. Dalam konteks metodologi hukum Indonesia, penelitian normatif tidak terbatas pada inventarisasi peraturan, tetapi mencakup penalaran sistematis untuk menemukan jawaban preskriptif terhadap persoalan hukum yang muncul.[12]

Penelitian menggunakan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan hukum. Pendekatan perundang-undangan digunakan untuk mengonstruksikan hubungan antara tindak pidana terhadap proses peradilan dalam KUHP Nasional dengan rezim pembuktian elektronik dalam KUHAP. Pendekatan konseptual diarahkan pada konsep *obstruction of justice*, *adversarial manipulation*, *anti-forensics*, autentisitas, reliabilitas, *mens rea*, dan kausalitas. Pendekatan kasus digunakan untuk membaca perkembangan argumentasi konstitusional mengenai batas kriminalisasi tindak pidana terhadap proses peradilan dan perubahan rezim pembuktian. Sementara itu, perbandingan hukum digunakan secara fungsional untuk menguji bagaimana perkembangan regulasi internasional membangun standar akurasi, transparansi, ketahanan, dan pengawasan manusia terhadap AI pada sektor penegakan hukum.

---

[10] Sandoval, M.-P., et al. (2024). Threat of deepfakes to the criminal justice system. https://doi.org/10.1186/s40163-024-00239-1; Azis, M. A., et al. (2026). Reconstructing reliability standards for deepfake detectors. https://doi.org/10.58812/wslhr.v4i03.3022; Capra, D. J. (2024). Deepfakes reach the advisory committee on evidence rules. https://ir.lawnet.fordham.edu/flr/vol92/iss6/7/; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651.

[11] Republik Indonesia. (2023). UU No. 1 Tahun 2023, Pasal 278, 281, dan 282. https://www.peraturan.go.id/files/uu1-2023.pdf; Republik Indonesia. (2025). UU No. 20 Tahun 2025, Pasal 235. https://peraturan.go.id/id/uu-no-20-tahun-2025; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651.

[12] Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. Audito Comparative Law Journal, 4(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Penggabungan beberapa pendekatan tersebut diperlukan karena persoalan yang diteliti terletak pada pertemuan hukum pidana, hukum pembuktian, dan karakter teknis sistem AI.[13]

Bahan hukum penelitian terdiri atas bahan hukum primer dan sekunder. Bahan hukum primer mencakup ketentuan hukum pidana dan hukum acara pidana yang berkaitan dengan penyesatan serta perintangan proses peradilan, putusan Mahkamah Konstitusi yang berkaitan dengan *obstruction of justice* dan pembuktian dalam KUHAP baru, serta instrumen regulasi AI yang relevan sebagai bahan perbandingan. Bahan hukum sekunder terdiri atas artikel jurnal hukum, literatur digital forensik, penelitian mengenai *adversarial machine learning*, *anti-forensics*, *deepfake detection*, *procedural due process*, dan tata kelola AI yang terbit terutama pada periode 2023–2026. Pemilihan bahan dilakukan berdasarkan relevansi substantif, kebaruan, keterlacakan sumber, dan keterhubungannya dengan rumusan masalah, bukan semata-mata berdasarkan kesamaan istilah dengan objek penelitian.[14]

Analisis dilakukan melalui empat tahap. Pertama, penelitian mengidentifikasi karakter teknis manipulasi adversarial untuk membedakannya dari pemalsuan digital biasa. Kedua, karakter tersebut dipetakan terhadap unsur perbuatan dan kepentingan hukum yang dilindungi oleh ketentuan tindak pidana terhadap proses peradilan. Ketiga, penelitian menguji hubungan antara tindakan manipulatif, kesengajaan pelaku, akibat terhadap proses pembuktian, serta batas interpretasi yang diperkenankan oleh asas legalitas. Keempat, hasil analisis digunakan secara preskriptif untuk merumuskan *Adversarial Evidence Interference Test* sebagai parameter untuk menentukan kapan serangan terhadap bukti atau sistem AI forensik dapat dikualifikasikan sebagai manipulasi alat bukti, perintangan proses peradilan, tindak pidana siber, atau kombinasi di antaranya. Pola analisis tersebut tetap menempatkan interpretasi gramatikal dan sistematis sebagai batas awal, sehingga rekonstruksi hukum tidak berubah menjadi penggunaan analogi yang memperluas pemidanaan.[15]

HASIL DAN PEMBAHASAN

Manipulasi Adversarial sebagai Bentuk Baru Intervensi terhadap Proses Pembuktian

Hasil analisis menunjukkan bahwa *adversarial manipulation* memiliki karakter yang berbeda dari pemalsuan bukti elektronik konvensional. Dalam pemalsuan biasa, pelaku mengubah substansi gambar, video, suara, atau dokumen agar informasi yang ditampilkan menyimpang dari keadaan sebenarnya. Sebaliknya, manipulasi adversarial dapat mempertahankan tampilan yang hampir sama bagi manusia, tetapi memasukkan pola yang mengubah cara model AI mengklasifikasikan bukti. Chen et al. (2024) dan Cirillo et al. (2025) meneliti kerentanan serta pengujian ketahanan *deepfake detector* terhadap *adversarial perturbations*. Temuan teknis ini memperlihatkan kemungkinan pengaruh terhadap proses inferensi, tetapi tidak membuktikan bahwa serangan semacam itu telah terjadi dalam perkara pidana tertentu.[16]

Perkembangan *anti-forensic deepfake* mempertegas perbedaan tersebut. Sampel adversarial dapat dirancang untuk menyembunyikan artefak pemalsuan sehingga sistem klasifikasi yang sebelumnya mampu membedakan media autentik dan palsu justru menilai objek hasil manipulasi sebagai autentik. Zhu dan Long menemukan bahwa teknik *anti-forensic* menimbulkan masalah karena sistem deteksi biner konvensional tidak selalu mengenali manipulasi yang sengaja dibuat untuk menghindari deteksi. Temuan ini memiliki implikasi langsung bagi hukum pembuktian. Apabila alat forensik berbasis AI digunakan untuk

[13] Choudhary, K. (2024). Which method should I select for my legal research? Teisė, 132, 135–144. https://doi.org/10.15388/Teise.2024.132.10.

[14] Majeed, N., Hilal, A., & Khan, A. N. (2023). Doctrinal research in law: Meaning, scope and methodology. Bulletin of Business and Economics, 12(4), 559–563. https://doi.org/10.61506/01.00167

[15] Choudhary, K. (2024). Which method should I select for my legal research? Teisė, 132, 135–144. https://doi.org/10.15388/Teise.2024.132.10.

[16] Chen, P., et al. (2024). DeepFake detection against adversarial examples. IET Image Processing, 18(3), 615–626. https://doi.org/10.1049/ipr2.12973; Cirillo, L., Gervasio, A., & Amerini, I. (2025). Explainability-driven adversarial robustness assessment for generalized deepfake detectors. https://doi.org/10.1186/s13635-025-00211-9.

menentukan integritas rekaman, maka pelaku tidak lagi harus menghapus rekaman untuk mengganggu pembuktian. Pelaku cukup merekayasa bagaimana sistem yang memeriksa rekaman tersebut akan menginterpretasikannya.[17]

Fenomena tersebut dapat ditempatkan dalam kerangka *anti-forensics* yang lebih luas. Kajian sistematis Surakanti, Goundar, dan Dwight menunjukkan bahwa *anti-forensics* mencakup berbagai teknik yang bertujuan menghambat, mengaburkan, memanipulasi, atau menyesatkan proses investigasi digital, termasuk *artifact wiping*, penyembunyian data, pengaburan jejak, dan serangan terhadap alat forensik itu sendiri. Perspektif ini penting karena menggeser pusat analisis dari pertanyaan "apakah bukti telah diubah?" menuju pertanyaan yang lebih luas, yaitu "apakah suatu tindakan secara sengaja mengurangi kemampuan proses forensik untuk memperoleh kesimpulan yang benar?". Dalam perspektif hukum pidana, perubahan tersebut membentuk titik temu baru antara perlindungan integritas alat bukti dan perlindungan terhadap fungsi proses peradilan.[18]

Diferensiasi Pasal 278, Pasal 281, dan Pasal 282 KUHP terhadap Manipulasi Adversarial

Bab VI KUHP membedakan penyesatan proses peradilan dari tindakan lain yang mengganggu proses peradilan. Pasal 278 ayat (1) huruf a mengatur penggunaan bukti palsu, sedangkan huruf c mengatur perubahan atau penghilangan alat bukti. Pasal 281 menyasar tindakan yang ditujukan kepada pejabat yang menjalankan fungsi proses peradilan dengan maksud khusus yang disebutkan dalam pasal. Pasal 282 ayat (1) berkaitan dengan penyembunyian orang dan bantuan melarikan diri. Pengelompokan ini bersumber dari teks UU Nomor 1 Tahun 2023; pembahasan akademiknya dapat dibandingkan dengan Pettanasse et al. (2024). Putusan MK Nomor 163/PUU-XXIII/2025 digunakan hanya sejauh memuat pemetaan norma, bukan sebagai dasar untuk menambah unsur delik.[19]

Dari konstruksi tersebut, Pasal 278 secara tekstual mempunyai kedekatan paling kuat dengan manipulasi adversarial yang dilakukan langsung terhadap bukti elektronik. Jika pelaku mengubah data elektronik dengan *perturbation* tertentu sehingga karakter komputasional bukti berubah, unsur "mengubah" alat bukti dapat menjadi titik analisis utama sepanjang objek yang dimanipulasi telah memiliki kedudukan sebagai alat bukti atau berkaitan dengan proses peradilan sebagaimana dimaksud norma. Akan tetapi, konstruksi tersebut tidak dapat otomatis diterapkan pada setiap penggunaan teknologi deepfake. Penelitian mengenai kriminalisasi deepfake di Indonesia menunjukkan bahwa penggunaan teknologi tersebut dapat bersinggungan dengan berbagai kepentingan hukum dan jenis delik yang berbeda, sehingga penentuan norma harus mengikuti tujuan, objek, konteks, dan akibat konkret dari perbuatan pelaku.[20]

Pasal 281 KUHP mensyaratkan tindakan "menghalang-halangi, mengintimidasi, atau memengaruhi Pejabat", disertai maksud "memaksa atau membujuknya agar melakukan atau tidak melakukan tugasnya". Dengan demikian, kesalahan klasifikasi AI yang kebetulan mempersulit pekerjaan penyidik atau hakim belum cukup untuk menerapkan Pasal 281. Penuntut harus menguraikan tindakan yang benar-benar tertuju pada pejabat beserta maksud khusus yang disyaratkan norma. Serangan terhadap model AI tanpa hubungan yuridis tersebut tidak boleh diidentikkan dengan perintangan terhadap pejabat. Pembatasan ini konsisten dengan tuntutan kepastian unsur delik yang dibahas oleh Pettanasse et al. (2024) serta Yamin dan

[17] Zhu, M., & Long, J. (2025). Detecting anti-forensic deepfakes with identity-aware multi-branch networks. Frontiers in Big Data, 8, Article 1720525. https://doi.org/10.3389/fdata.2025.1720525.

[18] Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations. International Journal of Information Security, 24, Article 210. https://doi.org/10.1007/s10207-025-01131-y.

[19] Republik Indonesia. (2023). UU No. 1 Tahun 2023, Pasal 278, 281, dan 282. https://www.peraturan.go.id/files/uu1-2023.pdf; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651; Mahkamah Konstitusi Republik Indonesia. (2025). Putusan Nomor 163/PUU-XXIII/2025 (dipergunakan terbatas pada pemetaan norma). https://www.mkri.id/public/content/persidangan/putusan/putusan_mkri_13289_1760599508.pdf.

[20] Al Alif, S. S., Rindiani, A., & Marhayati, C. (2025). Konstruksi hukum pidana dalam penanggulangan kejahatan siber berbasis teknologi deepfake di Indonesia. Legal Standing: Jurnal Ilmu Hukum, 9(5), 1169–1183. https://doi.org/10.24269/ls.v9i5.12406.

Bawono (2025), dan sejalan secara konseptual dengan kehati-hatian MK terhadap konstruksi perintangan yang terlalu elastis dalam Putusan Nomor 71/PUU-XXIII/2025.[21]

Pasal 282 ayat (1) huruf a KUHP memuat tindakan "menyembunyikan orang yang melakukan Tindak Pidana", sedangkan huruf b memuat pemberian pertolongan agar orang yang melakukan tindak pidana dapat melarikan diri dari penyidikan, penuntutan, atau pelaksanaan putusan pidana. Karena itu, manipulasi AI baru relevan terhadap Pasal 282 jika terbukti menjadi bagian dari penyembunyian atau pertolongan kepada orang sebagaimana dirumuskan pasal. Serangan atas alat analitik semata tidak otomatis memenuhi rumusan tersebut. Batas ini menegaskan bahwa perubahan bukti, tindakan terhadap pejabat, dan bantuan kepada pelaku merupakan kategori perbuatan berbeda yang memerlukan pembuktian terpisah.[22]

Karakter perbuatan	Titik normatif utama	Parameter pembeda
Mengubah bukti elektronik agar AI salah membaca autentisitas	Pasal 278	Perubahan ditujukan terhadap alat bukti atau benda yang mempunyai fungsi pembuktian
Membuat bukti AI-generated untuk digunakan menyesatkan proses hukum	Pasal 278	Ada penciptaan atau penggunaan bukti palsu dalam proses peradilan
Menyerang sistem AI dengan tujuan memengaruhi tindakan pejabat tertentu	Pasal 281 dapat dianalisis jika unsur lain terpenuhi	Harus terdapat hubungan dengan tindakan menghalangi, mengintimidasi, atau memengaruhi pejabat serta maksud khusus sebagaimana dirumuskan pasal
Membantu pelaku menghindari proses hukum melalui sarana digital	Pasal 282 dapat relevan menurut fakta konkret	Orientasi perbuatannya berupa penyembunyian atau pertolongan kepada pelaku
Serangan siber terhadap AI tanpa hubungan dengan proses peradilan	Tidak otomatis merupakan *obstruction of justice*	Harus dianalisis berdasarkan delik siber atau delik lain yang relevan

Asas Legalitas sebagai Batas Rekonstruksi *Obstruction of Justice*

Rekonstruksi hukum terhadap teknologi baru harus dibedakan dari penciptaan delik melalui analogi. Fakta bahwa suatu *adversarial attack* secara fungsional dapat menghambat penyidikan tidak dengan sendirinya memberikan dasar untuk memperluas unsur delik yang tidak mencakup perbuatan tersebut. Problem ini penting karena penelitian mengenai kriminalisasi kejahatan berbasis deepfake di Indonesia masih menemukan ketergantungan pada interpretasi

[21] Republik Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023, Pasal 281 (unsur tindakan terhadap pejabat dan maksud khusus). https://www.peraturan.go.id/files/uu1-2023.pdf; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651; Yamin, M., & Bawono, B. T. (2025). Law enforcement against obstruction of justice. https://doi.org/10.30659/jhku.v20i2.46094; Mahkamah Konstitusi Republik Indonesia. (2026c). Putusan Nomor 71/PUU-XXIII/2025 (berlaku atas UU Tipikor, bukan putusan tentang Pasal 281 KUHP).

[22] Republik Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023, Pasal 282 ayat (1) huruf a dan b (penyembunyian orang dan bantuan melarikan diri). https://www.peraturan.go.id/files/uu1-2023.pdf; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651 .

sejumlah ketentuan yang tidak sejak awal dirancang untuk manipulasi berbasis AI. Kondisi tersebut berpotensi menimbulkan ketegangan antara kebutuhan adaptasi hukum dan tuntutan *lex certa* serta *lex stricta*. Karena itu, rekonstruksi dalam penelitian ini tidak diarahkan untuk menyatakan bahwa semua serangan adversarial merupakan *obstruction of justice*, tetapi untuk menemukan batas tekstual dan fungsional tempat norma yang sudah ada dapat diterapkan secara sah.[23]

Batas tersebut dapat dibangun melalui tiga lapis pengujian. Pertama, harus terdapat actus reus yang mempunyai hubungan dengan bentuk perbuatan yang secara eksplisit dicantumkan dalam delik terkait. Kedua, harus terbukti keadaan batin atau tujuan yang disyaratkan oleh masing-masing rumusan, sehingga kesalahan teknis, kegagalan model, atau modifikasi data yang tidak disengaja tidak berubah menjadi tindak pidana. Ketiga, harus terdapat hubungan yang dapat dijelaskan antara perbuatan dan kepentingan proses peradilan yang hendak dilindungi. Model tersebut menjaga keseimbangan antara kebutuhan menghadapi modus teknologi baru dan prinsip bahwa kriminalisasi tidak dapat dibangun hanya berdasarkan kesamaan akibat. Kajian terbaru tentang asas legalitas KUHP Nasional juga menekankan pentingnya kepastian norma dan pencegahan interpretasi pidana yang subjektif ketika hukum menghadapi perkembangan sosial baru.[24]

Dari Autentisitas Bukti Menuju Reliabilitas Proses Autentikasi

Persoalan berikutnya muncul dalam ranah hukum acara. Bukti elektronik memiliki sifat yang mudah direplikasi dan dimodifikasi sehingga integritasnya sangat bergantung pada prosedur forensik yang dapat dilacak. Penelitian Agatha dan Rahaditya menunjukkan bahwa standar digital forensik dalam pembuktian pidana Indonesia masih terfragmentasi, padahal digital forensik menentukan autentisitas, integritas, dan reliabilitas bukti elektronik. Masalah tersebut menjadi lebih kompleks ketika AI berfungsi sebagai alat bantu autentikasi. Dalam situasi ini, pemeriksaan tidak cukup menilai apakah file yang diperlihatkan di persidangan sama dengan file yang diperoleh penyidik. Pemeriksaan juga harus menilai apakah sistem analitik yang memproses file tersebut tahan terhadap manipulasi yang sengaja dirancang untuk menghasilkan klasifikasi keliru.[25]

Dengan demikian, autentisitas dan reliabilitas harus dipisahkan secara konseptual. Autentisitas menjawab apakah objek yang diperiksa benar berasal dari sumber atau keadaan yang diklaim, sedangkan reliabilitas menilai apakah metode yang digunakan untuk menghasilkan kesimpulan terhadap objek tersebut cukup dapat dipercaya. Vanessa dan Firmansyah menunjukkan bahwa kerentanan bukti elektronik terhadap manipulasi menuntut pemenuhan aspek formal dan material, termasuk autentikasi dan pemeriksaan digital forensik. Dalam perkara yang melibatkan AI, standar tersebut perlu dikembangkan satu lapis lebih jauh. Bukti dapat tetap mempunyai nilai hash yang konsisten sejak penyitaan, tetapi kesimpulan AI atas bukti itu tetap tidak reliabel apabila model rentan terhadap *adversarial input*. Karena itu, *chain of custody* atas file harus dilengkapi dengan *chain of analytical reliability* atas proses yang mengubah data mentah menjadi kesimpulan forensik.[26]

Gagasan tersebut memperoleh dukungan dari perkembangan doktrin internasional. Stoykova mengembangkan konsep *right to procedural accuracy* dalam pengolahan bukti digital, yang mencakup perlindungan terhadap pemrosesan bukti yang tidak reliabel, akses terhadap rantai bukti, penjelasan, bantuan forensik, serta kesempatan untuk berpartisipasi pada tahap pemrosesan digital yang menentukan. Pendekatan ini penting untuk konteks manipulasi

[23] Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake sebagai bentuk kejahatan siber baru. Jurnal USM Law Review, 8(3), 2421–2445. https://doi.org/10.26623/julr.v8i3.13060.

[24] Nugraha, R. S., & Silalahi, C. F. (2024). Pembaharuan berlakunya asas legalitas dalam UU Nomor 1 Tahun 2023. PALAR (Pakuan Law Review), 10(1), 73–81. https://journal.unpak.ac.id/index.php/palar/article/view/10164.

[25] Agatha, C., & Rahaditya, R. (2026). Fragmented digital forensic standards in Indonesian criminal evidence. Indonesian Journal of Law and Economics Review, 21(2). https://doi.org/10.21070/ijler.v21i2.1558.

[26] Vanessa, V., & Firmansyah, H. (2025). Analysis of the validity of electronic evidence in criminal trial proceedings. Indonesian Journal of Law and Economics Review, 20(4). https://doi.org/10.21070/ijler.v20i4.1395

adversarial karena kesalahan pembuktian tidak selalu berasal dari bukti yang palsu. Kesalahan dapat muncul karena proses analitik yang tidak cukup kuat terhadap serangan, tidak dapat diuji ulang, atau tidak memberikan kesempatan kepada pihak yang terkena dampak untuk mempertanyakan metodologi yang digunakan.[27]

Dimensi *due process* juga mengharuskan keluaran AI tidak diperlakukan sebagai kesimpulan yang memiliki otoritas sendiri. Garrett menegaskan bahwa penggunaan AI oleh negara tidak menghilangkan tuntutan prosedural mengenai pemberitahuan, kesempatan untuk membantah, interpretabilitas, pengujian, dan reliabilitas. Konsekuensinya dalam hukum pembuktian pidana adalah bahwa terdakwa harus mempunyai kesempatan yang bermakna untuk mempertanyakan bagaimana suatu kesimpulan berbasis AI terbentuk, terutama apabila keluaran tersebut memengaruhi penilaian terhadap bukti yang menentukan kebebasannya. Sistem yang tidak memungkinkan pemeriksaan terhadap metode, parameter, tingkat kesalahan, atau keterbatasannya berpotensi menciptakan ketimpangan epistemik antara penegak hukum dan terdakwa.[28]

Adversarial Robustness sebagai Standar Baru Bukti yang Dianalisis dengan AI

Hasil penelitian menunjukkan bahwa salah satu unsur yang belum cukup diperhatikan oleh hukum pembuktian konvensional adalah *adversarial robustness,* yaitu kemampuan model untuk mempertahankan kinerja yang dapat dipercaya ketika menghadapi input yang sengaja dimodifikasi untuk mengecohnya. Cirillo, Gervasio, dan Amerini memperlihatkan bahwa ketahanan tersebut dapat diuji melalui serangan yang diarahkan pada bagian citra yang paling relevan bagi proses klasifikasi model. Temuan ini menunjukkan bahwa angka akurasi model dalam kondisi normal tidak cukup untuk menilai kelayakannya dalam proses peradilan. Sistem dengan akurasi tinggi pada dataset biasa dapat tetap mempunyai nilai forensik yang rendah jika sedikit perubahan adversarial mampu membalik kesimpulannya.[29]

Karena itu, pemeriksaan bukti elektronik berbasis AI seharusnya setidaknya menilai identitas dan versi model, sumber serta relevansi data pengujian, tingkat kesalahan, kemampuan generalisasi terhadap data yang tidak dikenal, *adversarial robustness*, keterlacakan proses analisis, dan kemungkinan reproduksi hasil oleh pemeriksa independen. Prinsip tersebut konsisten dengan perkembangan digital forensik yang menempatkan validasi, integritas data, *chain of custody*, dan pelaporan metode sebagai unsur penting ketika AI dan machine learning digunakan dalam investigasi. Sistem AI tidak boleh menggantikan penalaran forensik, melainkan harus menghasilkan keluaran yang dapat diaudit dan dipertanggungjawabkan.[30]

Pendekatan perbandingan memperkuat kebutuhan pengujian teknis, dengan tetap membedakan hukum Uni Eropa dan hukum Indonesia. Pasal 6 ayat (2) Regulation (EU) 2024/1689, dibaca bersama Annex III angka 6(c), memasukkan sistem AI yang dipakai oleh atau untuk otoritas penegak hukum guna mengevaluasi reliabilitas bukti dalam penyidikan atau penuntutan sebagai kategori AI berisiko tinggi, sepanjang syarat regulasinya terpenuhi. Pasal 15 menetapkan tuntutan mengenai akurasi, ketahanan, dan keamanan siber. Namun, penerapannya berlangsung bertahap: setelah perubahan oleh Regulation (EU) 2026/1744, ketentuan utama Chapter III Sections 1–3 untuk sistem Annex III berlaku mulai 2 Desember 2027, bukan seluruhnya mulai 2026. Kerangka ini merupakan pembanding fungsional bagi rancangan standar pembuktian Indonesia dan tidak secara langsung mengikat pengadilan Indonesia.[31]

---

[27] Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. Computer Law & Security Review, 55, 106040. https://doi.org/10.1016/j.clsr.2024.106040.

[28] Garrett, B. L. (2025). Artificial intelligence and procedural due process (Duke Law School Public Law & Legal Theory Series No. 2025-15). https://doi.org/10.2139/ssrn.5093989.

[29] Cirillo, L., Gervasio, A., & Amerini, I. (2025). Explainability-driven adversarial robustness assessment for generalized deepfake detectors. EURASIP Journal on Information Security, 2025, Article 23. https://doi.org/10.1186/s13635-025-00211-9.

[30] Mangrulkar, R., Pravin, H., & Pravin, S. (2024). Digital forensics in the age of AI and ML: Evidence handling, validation and reporting. Open Access Journal of Data Science and Artificial Intelligence, 2(1), 1–5. https://doi.org/10.23880/oajda-16000132.

[31] European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689, Pasal 6 ayat (2), Pasal 15, dan Annex III angka 6(c) [evaluasi reliabilitas bukti; bukan angka 6(b)]. https://eur-

Prinsip yang serupa terlihat dalam Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law tahun 2024. Konvensi tersebut menempatkan transparansi, pengawasan, akuntabilitas, tanggung jawab, reliabilitas, serta perlindungan prosedural sebagai prinsip dalam siklus hidup AI. Salah satu implikasinya ialah kebutuhan menyediakan informasi yang cukup agar individu dapat menggugat keputusan atau penggunaan sistem AI yang secara signifikan memengaruhi haknya. Bagi hukum pembuktian Indonesia, pendekatan ini mendukung gagasan bahwa legitimasi penggunaan AI tidak dapat bergantung hanya pada legalitas perolehan bukti. Sistem yang membantu menentukan makna suatu bukti juga harus mempunyai reliabilitas yang dapat dipertanggungjawabkan.[32]

Rekonstruksi *Adversarial Evidence Interference Test*

Berdasarkan analisis normatif dan teknis tersebut, penelitian ini menawarkan *Adversarial Evidence Interference Test* atau *AEIT* sebagai konstruksi untuk menilai apakah manipulasi terhadap bukti atau sistem AI telah memasuki wilayah tindak pidana terhadap proses peradilan. AEIT tidak dirancang sebagai unsur delik baru, tetapi sebagai perangkat analitis untuk menghubungkan fakta teknis dengan unsur hukum yang telah tersedia. Konstruksi ini penting agar pengadilan tidak langsung menyimpulkan adanya *obstruction of justice* hanya karena sebuah sistem AI diserang, sekaligus mencegah manipulasi teknologi yang nyata-nyata ditujukan untuk menyesatkan pembuktian lolos dari analisis hukum hanya karena modus tersebut belum dikenal ketika rumusan pidana dirancang.[33]

AEIT terdiri atas lima parameter yang bekerja secara berurutan. Pertama, *judicial-process nexus*, yakni bukti atau sistem yang menjadi sasaran harus mempunyai hubungan nyata dengan penyelidikan, penyidikan, penuntutan, pemeriksaan persidangan, atau pelaksanaan putusan. Kedua, *adversarial act,* yaitu terdapat intervensi teknis yang dapat diidentifikasi, seperti modifikasi input, penyisipan *perturbation*, pengubahan data, serangan terhadap alat forensik, atau tindakan anti-forensik lain. Ketiga, *knowledge and purpose*, pelaku mengetahui karakter manipulatif tindakan dan menghendaki penggunaannya untuk menyesatkan atau mengganggu proses pembuktian. Keempat, *material interference capability,* manipulasi secara objektif mempunyai kemampuan yang berarti untuk menghasilkan kesalahan klasifikasi atau mengurangi reliabilitas pemeriksaan. Kelima, *forensic causal traceability*, terdapat jalur teknis yang dapat diuji antara tindakan pelaku dan perubahan keluaran analitik. Kelima parameter tersebut memisahkan manipulasi yang mempunyai relevansi pidana dari kegagalan sistem, *false positive*, *false negative*, atau ketidakakuratan algoritma yang timbul tanpa perbuatan manusia yang memenuhi unsur kesalahan.[34]

Parameter kelima, *forensic causal traceability*, menuntut pembuktian kausalitas teknis yang dapat diuji, bukan sekadar urutan waktu antara modifikasi file dan keluaran AI yang keliru. Pemeriksa perlu (1) mengamankan input asli serta input yang diduga termodifikasi beserta nilai hash dan *chain of custody*; (2) menjalankan uji kontrafaktual pada model, versi, konfigurasi, dan ambang keputusan yang sama untuk membandingkan keluaran kedua input; (3) mengulang pengujian pada beberapa percobaan serta, bila memungkinkan, mereplikasinya dengan alat dan pemeriksa independen; dan (4) membandingkan selisih kesalahan dengan *error rate* dasar, *false-positive rate*, dan *false-negative rate* pada data pembanding yang relevan. Dokumentasi perubahan skor, log, dan kondisi pengujian diperlukan untuk memisahkan dampak manipulasi

lex.europa.eu/eli/reg/2024/1689/oj; European Parliament & Council of the European Union. (2026). Regulation (EU) 2026/1744, perubahan Pasal 113: kewajiban utama Chapter III Sections 1–3 bagi AI high-risk Annex III berlaku 2 Desember 2027; Annex I berlaku 2 Agustus 2028. https://eur-lex.europa.eu/eli/reg/2026/1744/oj

[32] Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225.

[33] Rajendra, J. B., & Thuraisingam, A. S. (2026). The role of explainability and human intervention in AI decisions. Information & Communications Technology Law, 35(2), 152–183. https://doi.org/10.1080/13600834.2025.2537514.

[34] Zhu, M., & Long, J. (2025). Detecting anti-forensic deepfakes. https://doi.org/10.3389/fdata.2025.1720525; Surakanti, S., et al. (2025). Countering anti-forensic tactics. https://doi.org/10.1007/s10207-025-01131-y.

dari variasi normal sistem. Pada model *black-box* atau sistem berpemilik yang tidak membuka bobot, data pelatihan, maupun log yang cukup, pengujian hanya mungkin menilai keterulangan keluaran dan hubungan empiris yang terbatas; atribusi mekanisme internal tidak boleh dipastikan tanpa bukti pendukung. Metode ini merupakan usulan operasional AEIT berdasarkan prinsip validasi forensik dan literatur *anti-forensics*, bukan protokol yang telah diuji secara empiris dalam penelitian ini.[35]

Rekonstruksi Dua Lapis: Hukum Pidana Materiil dan Hukum Pembuktian

Rekonstruksi yang dihasilkan penelitian ini bekerja pada dua lapis yang berbeda tetapi saling berhubungan. Pada lapis hukum pidana materiil, penegak hukum harus menentukan apakah tindakan pelaku secara tekstual memenuhi perbuatan yang dirumuskan dalam Pasal 278, Pasal 281, Pasal 282, atau ketentuan pidana lain. Pada lapis hukum acara, pengadilan harus menentukan apakah bukti elektronik dan hasil analisis AI yang digunakan untuk membuktikan tindakan tersebut autentik, reliabel, dapat dilacak, dan dapat diuji oleh pihak lawan. Pemisahan ini penting. Bukti yang menunjukkan adanya serangan adversarial belum otomatis membuktikan *mens rea*, sedangkan terpenuhinya *mens rea* tidak dapat menggantikan kebutuhan untuk membuktikan secara teknis bahwa serangan benar-benar terjadi.[36]

Putusan MK Nomor 111/PUU-XXIV/2026, diucapkan pada 12 Mei 2026, berkenaan dengan pengujian Pasal 235 ayat (1) huruf e KUHAP tentang barang bukti sebagai kategori alat bukti mandiri, bukan huruf f tentang bukti elektronik. Mahkamah menyatakan permohonan tidak dapat diterima karena para pemohon tidak membuktikan kedudukan hukum yang diperlukan. Oleh sebab itu, putusan tersebut tidak mengandung penilaian pokok tentang konstitusionalitas norma dan tidak dapat ditafsirkan sebagai pengesahan maupun penolakan standar autentikasi bukti elektronik atau analisis AI. Perkara tersebut disebut hanya sebagai konteks adanya perdebatan atas klasifikasi alat bukti. Dasar utama pembahasan reliabilitas bukti elektronik tetap berada pada Pasal 235 ayat (1) huruf f serta ayat (3)–(5) KUHAP dan literatur forensik yang relevan.[37]

Pada tataran prosedural, penelitian ini karena itu mengusulkan agar hasil analisis AI terhadap bukti elektronik dinilai melalui *provenance, integrity, model transparency, validation, error rate, adversarial robustness, reproducibility, dan human oversight.* Parameter tersebut tidak berarti hakim harus menjadi ahli machine learning. Pengadilan cukup menuntut agar pihak yang mengajukan hasil analisis dapat menjelaskan asal-usul bukti, metode pemeriksaan, versi alat, batas kemampuan sistem, hasil validasi, kemungkinan kesalahan, dan apakah analisis independen menghasilkan kesimpulan serupa. Pendekatan tersebut menempatkan teknologi sebagai objek yang diuji oleh hukum, bukan sebagai otoritas yang menentukan kebenaran di luar proses pembuktian.[38]

Implikasi Rekonstruksi terhadap Konsep *Obstruction of Justice* Berbasis AI

Temuan penelitian akhirnya menunjukkan bahwa *obstruction of justice* pada era AI perlu dipahami berdasarkan fungsi yang dilindungi hukum, tanpa menghapus batas tekstual setiap delik. Teknologi memungkinkan pelaku mengganggu proses peradilan tanpa menyentuh penyidik, saksi, atau benda bukti secara fisik. Ia dapat menyerang lapisan komputasional yang

[35] Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics. https://doi.org/10.1007/s10207-025-01131-y; Chen, P., Xu, M., & Qi, J. (2024). DeepFake detection against adversarial examples. https://doi.org/10.1049/ipr2.12973; Stoykova, R. (2024). A new right to procedural accuracy. https://doi.org/10.1016/j.clsr.2024.106040.

[36] Stoykova, R. (2024). A new right to procedural accuracy. https://doi.org/10.1016/j.clsr.2024.106040; Garrett, B. L. (2025). Artificial intelligence and procedural due process. https://doi.org/10.2139/ssrn.5093989.

[37] Mahkamah Konstitusi Republik Indonesia. (2026b). Putusan Nomor 111/PUU-XXIV/2026 (diucapkan 12 Mei 2026), pengujian Pasal 235 ayat (1) huruf e (barang bukti) UU No. 20 Tahun 2025. Amar: permohonan tidak dapat diterima karena kedudukan hukum; tidak ada pemeriksaan pokok norma. https://www.mkri.id/berita/pemohon-tak-dapat-menjelaskan-kerugian-konstitusional-uji-kuhap-25047

[38] Rajendra, J. B., & Thuraisingam, A. S. (2026). The role of explainability and human intervention in AI decisions. https://doi.org/10.1080/13600834.2025.2537514; Mangrulkar, R., et al. (2024). Digital forensics in the age of AI and ML. https://doi.org/10.23880/oajda-16000132.

menentukan bagaimana bukti dipersepsikan. Namun perubahan modus tersebut tidak membenarkan perluasan seluruh tindakan menjadi Pasal 281. Jika serangan diarahkan pada substansi atau fungsi pembuktian suatu alat bukti, Pasal 278 mempunyai kedekatan normatif yang lebih kuat. Pasal 281 baru relevan ketika unsur tindakan terhadap pejabat dan maksud khusus yang ditentukan undang-undang dapat dibuktikan. Sementara itu, Pasal 282 tetap memerlukan konteks bantuan atau penyembunyian pelaku. Diferensiasi inilah yang menjaga rekonstruksi tetap adaptif sekaligus konsisten dengan asas legalitas.[39]

Kebaruan penelitian ini dengan demikian berada pada pergeseran dari paradigma "bukti palsu" menuju "interferensi terhadap kemampuan sistem pembuktian menemukan kebenaran". Rekonstruksi tidak hanya melindungi integritas objek elektronik, tetapi juga integritas proses analitik yang menentukan nilai objek tersebut. AEIT kemudian berfungsi sebagai penghubung antara hukum pidana materiil dan digital forensik: hukum menentukan unsur yang harus dibuktikan, sedangkan ilmu forensik menjelaskan apakah manipulasi benar-benar terjadi, bagaimana mekanismenya bekerja, dan apakah manipulasi tersebut mempunyai kemampuan material untuk memengaruhi proses pembuktian. Model ini memungkinkan hukum Indonesia merespons modus adversarial secara lebih presisi tanpa menciptakan kriminalisasi melalui analogi dan tanpa memberikan kepercayaan berlebihan terhadap keluaran sistem.[40]

KESIMPULAN DAN SARAN

Pertanyaan pertama dijawab dengan pembedaan objek intervensi: pemalsuan digital konvensional mengubah informasi yang diterima manusia, sedangkan manipulasi adversarial dapat menargetkan proses inferensi AI sehingga kesimpulan forensik berubah tanpa perubahan visual yang mudah dikenali. Penilaian adanya serangan tetap membutuhkan bukti teknis tentang perubahan input, perilaku model, dan konteks pemakaiannya; kekeliruan algoritma dengan sendirinya bukan tindakan pidana.

Pertanyaan kedua dijawab secara normatif. Pasal 278 KUHP menjadi titik analisis utama apabila tindakan memenuhi unsur pemalsuan atau perubahan alat bukti dalam proses peradilan. Pasal 281 hanya relevan jika terbukti tindakan terhadap pejabat disertai maksud khusus untuk memaksa atau membujuknya, sedangkan Pasal 282 mensyaratkan penyembunyian atau pertolongan terhadap orang yang melakukan tindak pidana. Kesamaan akibat berupa terganggunya proses pembuktian tidak membenarkan penyamaan unsur delik atau analogi yang merugikan terdakwa.

Pertanyaan ketiga dijawab dengan rekonstruksi dua lapis. Pada lapis hukum acara, Pasal 235 ayat (1) huruf f serta ayat (3)–(5) KUHAP menjadi dasar untuk menguji autentikasi dan perolehan bukti elektronik. Pada lapis analitik, penelitian mengusulkan AEIT yang memeriksa hubungan dengan proses peradilan, tindakan adversarial, pengetahuan serta tujuan pelaku, kemampuan mengganggu pembuktian secara material, dan keterlacakan kausalitas forensik. Penilaian teknis mencakup uji kontrafaktual, replikasi independen, error rate dasar, keterbatasan model black-box, dan pemeriksaan ahli secara kontradiktor. AEIT adalah konstruksi analitis yang belum divalidasi pada perkara nyata atau pengujian laboratorium dan bergantung pada penafsiran teks pasal yang berlaku.

Sebagai tindak lanjut, Mahkamah Agung dan lembaga penegak hukum perlu mengembangkan pedoman pemeriksaan bukti berbasis AI yang menetapkan dokumentasi asal-usul dan integritas input, identitas serta versi model, protokol validasi, pengukuran tingkat kesalahan, pengujian adversarial, pengungkapan keterbatasan alat, dan kesempatan para pihak menguji hasilnya. Penelitian berikutnya perlu menguji AEIT pada simulasi forensik terkontrol dan putusan konkret, serta menilai kemampuan laboratorium, penyidik, jaksa, advokat, dan hakim

[39] Republik Indonesia. (2023). UU No. 1 Tahun 2023, Pasal 278, 281, dan 282. https://www.peraturan.go.id/files/uu1-2023.pdf; Pettanasse, I., et al. (2024). Tindak pidana "obstruction of justice". https://doi.org/10.61994/jsls.v2i2.651; Yamin, M., & Bawono, B. T. (2025). Law enforcement against obstruction of justice. https://doi.org/10.30659/jhku.v20i2.46094.

[40] Council of Europe. (2024). Framework Convention on Artificial Intelligence (CETS No. 225). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225; Stoykova, R. (2024). A new right to procedural accuracy. https://doi.org/10.1016/j.clsr.2024.106040

untuk menerapkannya. Sampai validasi tersebut tersedia, seluruh temuan artikel ini harus dipahami sebagai penalaran hukum normatif dan rancangan metodologis, bukan kesimpulan empiris mengenai efektivitas AEIT.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada seluruh pihak yang telah memberikan dukungan akademik, pemikiran, dan akses terhadap berbagai sumber hukum serta literatur yang digunakan dalam penelitian ini. Apresiasi juga disampaikan kepada para akademisi, peneliti, dan institusi yang mengembangkan kajian mengenai hukum pidana, bukti elektronik, digital forensik, serta *artificial intelligence*, sehingga penelitian ini dapat mengembangkan analisis lintas disiplin mengenai manipulasi adversarial dalam proses peradilan pidana. Segala kekurangan dalam penelitian ini sepenuhnya menjadi tanggung jawab penulis.

DAFTAR PUSTAKA

Agatha, C., & Rahaditya, R. (2026). Fragmented digital forensic standards in Indonesian criminal evidence. *Indonesian Journal of Law and Economics Review*, *21*(2). https://doi.org/10.21070/ijler.v21i2.1558.

Al Alif, S. S., Rindiani, A., & Marhayati, C. (2025). Konstruksi hukum pidana dalam penanggulangan kejahatan siber berbasis teknologi deepfake di Indonesia. *Legal Standing: Jurnal Ilmu Hukum*, *9*(5), 1169–1183. https://doi.org/10.24269/ls.v9i5.12406.

Antoro, H., Budhijanto, D., & Somawijaya. (2026). Admissibility of artificial intelligence as electronic evidence: Comparative perspectives from Indonesia, the United States, and Japan. *Jurnal IUS Kajian Hukum dan Keadilan*, *14*(1), 122–139. https://doi.org/10.29303/ius.v14i1.1880.

Azis, M. A., Pujiyono, & Putri, R. A. K. (2026). Reconstructing reliability standards for deepfake detectors as electronic evidence in Indonesia's criminal justice system. *West Science Law and Human Rights*, *4*(3), 299–309. https://doi.org/10.58812/wslhr.v4i03.3022.

Capra, D. J. (2024). Deepfakes reach the advisory committee on evidence rules. *Fordham Law Review*, *92*(6), 2491–2506. https://ir.lawnet.fordham.edu/flr/vol92/iss6/7/.

Chen, P., Xu, M., & Qi, J. (2024). DeepFake detection against adversarial examples based on D-VAEGAN. *IET Image Processing*, *18*(3), 615–626. https://doi.org/10.1049/ipr2.12973.

Choudhary, K. (2024). Which method should I select for my legal research: Doctrinal, empirical, multi-method or something else? *Teisė*, *132*, 135–144. https://doi.org/10.15388/Teise.2024.132.10

Cirillo, L., Gervasio, A., & Amerini, I. (2025). Explainability-driven adversarial robustness assessment for generalized deepfake detectors. *EURASIP Journal on Information Security*, *2025*, Article 23. https://doi.org/10.1186/s13635-025-00211-9.

Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225.

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Parliament & Council of the European Union. (2026). Regulation (EU) 2026/1744 of 8 July 2026 amending Regulation (EU) 2024/1689. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2026/1744/oj.

Garrett, B. L. (2025). Artificial intelligence and procedural due process (Duke Law School Public Law & Legal Theory Series No. 2025-15). Duke University School of Law. https://doi.org/10.2139/ssrn.5093989.

Hooda, A., Mangaokar, N., Feng, R., Fawaz, K., Jha, S., & Prakash, A. (2024). D4: Detection of adversarial diffusion deepfakes using disjoint ensembles. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (pp. 3812–3822). IEEE. https://doi.org/10.1109/WACV57701.2024.00377.

Jamil, A., & Saifuddin, S. (2026). The use of artificial intelligence in the court process in Indonesia: A review of procedural law on the aspect of evidence and decision-making. *Lex Scientia Law Review*, *10*(1), 521–550. https://doi.org/10.15294/lslr.v10i1.28681.

Mahkamah Konstitusi Republik Indonesia. (2025). Putusan Nomor 163/PUU-XXIII/2025. https://www.mkri.id/public/content/persidangan/putusan/putusan_mkri_13289_1760599508.pdf.

Mahkamah Konstitusi Republik Indonesia. (2026a, 2 Maret). MK hapus pasal karet "obstruction of justice". https://www.mkri.id/berita/mk-hapus-pasal-karet-%E2%80%9Cobstruction-of-justice%E2%80%9D-24696

Mahkamah Konstitusi Republik Indonesia. (2026b). Putusan Nomor 111/PUU-XXIV/2026 (12 Mei 2026). https://www.mkri.id/perkara/persidangan/putusan?search=111%2FPUU-XXIV%2F2026.

Mahkamah Konstitusi Republik Indonesia. (2026c). Putusan Nomor 71/PUU-XXIII/2025 (2 Maret 2026). https://www.mkri.id/perkara/persidangan/putusan?search=71%2FPUU-XXIII%2F2025.

Majeed, N., Hilal, A., & Khan, A. N. (2023). Doctrinal research in law: Meaning, scope and methodology. *Bulletin of Business and Economics*, *12*(4), 559–563. https://doi.org/10.61506/01.00167.

Mangrulkar, R., Pravin, H., & Pravin, S. (2024). Digital forensics in the age of AI and ML: Evidence handling, validation and reporting. *Open Access Journal of Data Science and Artificial Intelligence*, *2*(1), 1–5. https://doi.org/10.23880/oajda-16000132.

Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. *Audito Comparative Law Journal*, *4*(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Nugraha, R. S., & Silalahi, C. F. (2024). Pembaharuan berlakunya asas legalitas dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. *PALAR (Pakuan Law Review)*, *10*(1), 73–81. https://journal.unpak.ac.id/index.php/palar/article/view/10164.

Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake sebagai bentuk kejahatan siber baru: Tantangan kriminalisasi dalam hukum pidana Indonesia. *Jurnal USM Law Review*, *8*(3), 2421–2445. https://doi.org/10.26623/julr.v8i3.13060.

Pettanasse, I., Rani, F. H., Saputra, M. A., & Ardha, D. J. (2024). Tindak pidana "obstruction of justice" dalam pengaturan Undang-Undang Nomor 1 Tahun 2023. *Journal of Sharia and Legal Science*, *2*(2), 163–177. https://doi.org/10.61994/jsls.v2i2.651.

Rajendra, J. B., & Thuraisingam, A. S. (2026). The role of explainability and human intervention in AI decisions: Jurisdictional and regulatory aspects. *Information & Communications Technology Law*, *35*(2), 152–183. https://doi.org/10.1080/13600834.2025.2537514.

Republik Indonesia. (2023). Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (LN 2023 No. 1, TLN No. 6842). https://www.peraturan.go.id/files/uu1-2023.pdf.

Republik Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (LN 2025 No. 188, TLN No. 7149). https://peraturan.go.id/id/uu-no-20-tahun-2025.

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, *13*, Article 41. https://doi.org/10.1186/s40163-024-00239-1.

Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, *55*, 106040. https://doi.org/10.1016/j.clsr.2024.106040.

Sumardiana, B., Pujiyono, Cahyaningtyas, I., & Wulandari, C. (2024). Evaluation of electronic evidence in criminal justice in the era of advanced artificial intelligence technology. *Indonesian Journal of Criminal Law Studies*, *9*(2), 309–332. https://doi.org/10.15294/ijcls.v9i2.36634.

Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations: A systematic literature review. *International Journal of Information Security*, *24*, Article 210. https://doi.org/10.1007/s10207-025-01131-y.

Vanessa, V., & Firmansyah, H. (2025). Analysis of the validity of electronic evidence in criminal trial proceedings and the implementation of its admissibility. *Indonesian Journal of Law and Economics Review*, *20*(4). https://doi.org/10.21070/ijler.v20i4.1395.

Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2024). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2e2023). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2023.

Yamin, M., & Bawono, B. T. (2025). Law enforcement against obstruction of justice in eradicating criminal acts of corruption in Indonesia. *Jurnal Hukum Khaira Ummah*, *20*(2), 585–601. https://doi.org/10.30659/jhku.v20i2.46094.

Zhu, M., & Long, J. (2025). Detecting anti-forensic deepfakes with identity-aware multi-branch networks. *Frontiers in Big Data*, *8*, Article 1720525. https://doi.org/10.3389/fdata.2025.1720525.