CESSIE
Jurnal Ilmiah Hukum
Vol 4 No 2 Juli 2025
ISSN: 2830-0092 (Print) ISSN: 2830-0106 (Electronic)
Open Access: https://jurnal.arkainstitute.co.id/index.php/cessie/index

Tinjauan hukum tata negara terhadap kekosongan hukum digital forensik dalam penegakan hukum siber

Andi Arini Besse Lise[1], Irmanjaya Thaher[2]
[1,2]Universitas Esa Unggul
[1]abesselise@student.esaunggul.ac.id, [2]irman.jaya@esaunggul.ac.id

Info Artikel :
Diterima :
25 Mei 2025
Disetujui :
18 Juni 2025
Dipublikasikan :
14 Juli 2025

ABSTRAK

Perkembangan kejahatan siber di Indonesia menghadirkan tantangan baru dalam pembuktian hukum, terutama ketika pelaku menggunakan teknik anti-digital forensik seperti data wiping atau manipulasi jejak elektronik. Dalam konteks ini, peran aparat penegak hukum sangat penting untuk memastikan bahwa bukti elektronik dapat digunakan secara sah dalam proses peradilan. Namun demikian, Indonesia belum memiliki kerangka hukum khusus yang mengatur secara rinci tata cara digital forensik, baik dari sisi teknis maupun prosedural. Penelitian ini bertujuan untuk meninjau kekosongan hukum tersebut dalam perspektif Hukum Tata Negara, dengan menyoroti tanggung jawab konstitusional negara terhadap jaminan perlindungan hak atas keadilan dan kepastian hukum bagi warga negara. Metode yang digunakan adalah yuridis normatif dengan pendekatan konstitusional dan analisis terhadap peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa kekosongan hukum, ketidakjelasan norma, dan konflik antaraturan menjadi hambatan konstitusional dalam mewujudkan prinsip negara hukum sebagaimana tercantum dalam Pasal 1 ayat (3) UUD NRI 1945. Oleh karena itu, diperlukan reformasi regulasi dan penguatan kapasitas aparat hukum untuk menjamin efektivitas penegakan hukum siber secara konstitusional.

Kata Kunci: Anti Digital Forensik, Kredibilitas Bukti Elektronik, Kejahatan Siber, *Data Wiping*, Pendekatan Yuridis-Normatif

ABSTRACT

The development of cybercrime in Indonesia presents new challenges in legal proof, particularly when perpetrators employ anti-digital forensic techniques such as data wiping or the manipulation of electronic traces. In this context, the role of law enforcement is crucial to ensure that electronic evidence can be lawfully admitted in court proceedings. However, Indonesia still lacks a specific legal framework that comprehensively regulates digital forensics, both in technical and procedural terms. This study aims to examine this legal vacuum from a Constitutional Law perspective by highlighting the state's constitutional responsibility to guarantee the protection of the rights to justice and legal certainty for its citizens. The method used is normative juridical, employing a constitutional approach and analysis of statutory regulations. The findings show that the legal vacuum, normative ambiguity, and regulatory conflicts pose constitutional barriers to realizing the rule of law principle as stipulated in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia. Therefore, regulatory reform and capacity-building for law enforcement officers are necessary to ensure the constitutionally effective enforcement of cyber laws.

Keywords : Anti-Digital Forensics, Credibility of Electronic Evidence, Cybercrime, Data Wiping, Normative Juridical Approach

PENDAHULUAN

Perkembangan dalam teknologi informasi membawa perubahan yang signifikan dalam berbagai bidang kehidupan, termasuk dalam kejahatan siber. Dengan bertambahnya kompleksitas serangan siber, pihak penegak hukum menghadapi tantangan besar dalam mengidentifikasi dan menangani pelaku kejahatan. Salah satu kesulitan utama adalah praktik anti-digital forensik, di mana pelaku berusaha menghapus, menyembunyikan, atau memanipulasi bukti elektronik untuk menghindari hukum. Teknik seperti data wiping, yang bertujuan untuk menghapus jejak digital, menjadi kendala besar dalam pembuktian kasus. Selain keterangan dari saksi dan terdakwa yang bisa mempercepat pengungkapan beberapa jenis kejahatan, barang bukti digital juga sangat penting untuk memberikan

petunjuk dan memperjelas kejadian yang telah terjadi, terutama dalam kasus tindak pidana yang menggunakan teknologi informasi.[1]

Perdebatan mengenai kejahatan siber (*cybercrime*) masih hangat dibahas di kalangan akademisi hukum karena kejahatan ini tergolong fenomena baru yang terus berkembang. Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP) kerap menjadi titik sorotan baik dikritik maupun dipertahankan terkait sejauh mana relevansinya dalam menangani kasus- kasus cybercrime. Penegakan hukum terhadap pelaku kejahatan digital saat ini masih bergantung pada ketentuan dalam KUHP, khususnya pasal-pasal yang tidak lazim digunakan untuk jenis kejahatan ini. Hal ini memperlihatkan bahwa sistem hukum konvensional belum sepenuhnya mampu merespons kompleksitas serta dinamika perkembangan kejahatan siber yang terus berubah.[2]

Berbagai bentuk penyelidikan kini semakin berkembang untuk menjawab beragam kebutuhan investigasi. Praktisi forensik digital berperan di berbagai sektor masyarakat, baik di tingkat pemerintah pusat, daerah, hingga lembaga penegakan hukum lokal, perusahaan skala kecil, maupun korporasi internasional. Tiap-tiap sektor tersebut memiliki sistem aturan, kebijakan, serta prosedur hukum yang berbeda satu sama lain. Oleh karena itu, tantangan yang dihadapi para penyelidik forensik digital akan sangat tergantung pada jenis institusi, wilayah administratif, dan bahkan negara tempat mereka menjalankan tugas. Kondisi ini menegaskan bahwa keberhasilan dalam proses investigasi digital sangat erat kaitannya dengan kesesuaian regulasi dan kebijakan yang berlaku di masing- masing yurisdiksi.[3] Dalam proses persidangan, tahapan pembuktian memegang peranan krusial dalam mengungkap kebenaran atas suatu peristiwa atau hubungan hukum yang menjadi pokok sengketa. Tahapan ini digunakan oleh penggugat sebagai sarana untuk membuktikan adanya hak yang diklaim, yang menjadi dasar diajukannya gugatan. Melalui mekanisme pembuktian ini pula, hakim akan memperoleh pijakan yuridis dalam merumuskan putusan guna menyelesaikan perkara secara adil.[4]

Bukti digital harus dikumpulkan dan dianalisis dengan hati-hati agar dapat digunakan sebagai alat bukti yang sah di pengadilan.[5] Meskipun digital forensik telah menjadi instrumen penting dalam proses penyelidikan, Indonesia masih menghadapi kendala serius berupa belum adanya pedoman hukum yang spesifik dan memadai untuk menangani kejahatan siber, khususnya terhadap bukti elektronik yang dimanipulasi atau dihapus secara sistematis. Ketidakjelasan standar hukum terkait validitas dan kredibilitas bukti elektronik berpotensi melemahkan upaya penegakan hukum, terutama dalam menjamin bahwa hasil digital forensik dapat diterima sebagai alat bukti yang sah di pengadilan.

Permasalahan tersebut mencerminkan tiga problematika hukum yang sering terjadi dalam sistem hukum nasional, yakni: kekosongan hukum (*leemte in het recht*), ketidakjelasan hukum (*vagueness in law*), dan konflik norma (*norm conflict*). Kekosongan hukum terjadi ketika tidak ada aturan khusus yang mengatur digital forensik secara komprehensif; ketidakjelasan hukum terjadi karena aturan yang ada seperti dalam UU ITE belum memberikan panduan teknis yang memadai; dan konflik norma tampak dari ketidaksesuaian antara KUHAP dengan kebutuhan akan pengakuan bukti digital modern. Ketiga masalah ini secara langsung mempengaruhi efektivitas aparat penegak hukum dalam menjamin keadilan dan kepastian hukum.

Hak asasi manusia merupakan fondasi utama dalam sistem hukum Indonesia yang dijamin oleh UUD 1945, termasuk kebebasan untuk berserikat, berpendapat, dan memperjuangkan hak secara individu maupun kolektif. Namun, kebebasan tersebut tetap tunduk pada batasan demi menjaga ketertiban dan menghormati hak orang lain (Pasal 28J ayat (2). Dalam negara hukum, seperti ditegaskan A.V. Dicey dan Austin Ranney, supremasi hukum dan perlindungan hak harus dijamin secara konstitusional dan nondiskriminatif. Dalam konteks digital forensik, prinsip ini menjadi penting karena proses identifikasi dan pemeriksaan bukti digital harus tetap menjunjung tinggi hak privasi dan keadilan. Sebagaimana dikemukakan Mahfud MD, hukum sebagai produk politik harus diarahkan

---

[1] Synthiana Rachmie, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi* 21, no. 1 (2020): 104–27.

[2] Rafi Septia Budianto Pansariadi and Noenik Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (December 20, 2023): 287–98, https://doi.org/10.37893/jbh.v12i2.605.

[3] Agus Wibowo, *Digital Forensik* (Semarang: Penerbit Yayasan Prima Agus Teknik, 2023).

[4] Eddy Army, *Bukti Elektronik Dalam Praktik Peradilan* (Sinar Grafika, 2020).

[5] Sahat Parulian Sitorus et al., "Digital Cyber Forensics," *JURNAL ARJUNA* 1, no. 1 (2023): 7–10.

untuk melindungi kepentingan publik secara konstitusional, termasuk dalam merespons tantangan forensik digital di era siber.[6]

Sementara Indonesia masih mencari formulasi hukum yang ideal, negara-negara seperti Amerika Serikat dan Uni Eropa telah mengembangkan standar yang lebih mapan dalam bidang digital forensik. NIST Special Publication 800-61 tentang Computer Security Incident Handling Guide, Federal Rules of Evidence 902 tentang Evidence That Is Self- Authenticating, ENISA Guidelines dan ISO/IEC 27037:2019 menjadi acuan penting dalam memastikan integritas bukti elektronik. Selain dokumen Standar Nasional Indonesia yang menjadi rujukan dalam proses forensik digital di Indonesia, terdapat standardisasi yang banyak digunakan, yaitu dokumen NIST SP 800-86. Dokumen NIST SP 800-86 merupakan dokumen standardisasi yang dikeluarkan oleh Kementerian Perdagangan Amerika melalui National Institute of Standards and Technology (NIST) tentang petunjuk teknis forensik digital.[7] Panduan ini telah menjadi referensi penting bagi berbagai kalangan praktisi serta institusi penegak hukum di banyak negara dalam pelaksanaan tahapan identifikasi, pengumpulan, pemeriksaan, hingga analisis terhadap bukti digital secara terstruktur dan sah menurut hukum. Berdasarkan penjelasan sebelumnya, penelitian ini diarahkan pada analisis terhadap kekosongan hukum dalam pengaturan digital forensik, khususnya dalam konteks penanganan kejahatan siber yang melibatkan teknik anti-digital forensik seperti data wiping. Fokus penelitian ini adalah untuk menelaah kekosongan regulasi dari perspektif Hukum Tata Negara, dengan menitikberatkan pada tanggung jawab konstitusional negara dalam menjamin kepastian hukum, keadilan, dan perlindungan hak asasi warga negara.

Berlandaskan rincian permasalahan sebelumnya, penulis merasa tertarik untuk meneliti persoalan ini dalam perspektif hukum tata negara dengan judul: "Tinjauan Hukum Tata Negara terhadap Kekosongan Hukum Digital Forensik dalam Penegakan Hukum Siber di Indonesia". Penelitian ini diharapkan dapat memberikan kontribusi akademik dalam mengidentifikasi kebutuhan regulasi yang konstitusional, serta menjadi masukan dalam perumusan kebijakan hukum nasional yang adaptif terhadap tantangan teknologi informasi. dalam mendorong penyusunan regulasi yang konstitusional dan responsif terhadap tantangan teknologi dalam sistem hukum nasional.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang- undangan, perbandingan hukum, dan pendekatan konstitusional. Jenis data yang digunakan adalah sebagai berikut:

Bahan hukum primer merupakan sumber hukum utama yang mempunyai sifat autoritatif, yang mana bahan hukum yang mempunyai legitimasi atau kewenangan, seperti aturan perundang-undangan. Dalam konteks ini, beberapa Undang-undang yang digunakan peneliti yaitu di antaranya:

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008;
c. Kitab Undang-Undang Hukum Pidana (KUHP)
d. NIST Special Publication 800-61 tentang Computer Security Incident Handling Guide
e. Federal Rules of Evidence 902 tentang Evidence That Is Self-Authenticating
f. ENISA Guidelines dan ISO/IEC 27037:2019, NIST SP 800-86 Guide to
g. Integrating Forensic Techniques Into Incident Response

Bahan Hukum Sekunder adalah bahan hukum yang menjelaskan bahan hukum primer, meliputi:

a. Buku
b. Jurnal
c. Artikel Ilmiah yang membahas digital forensic, bukti elektronik, dan anti- digital forensic
d. Hasil penelitian yang membahas mengenai cybercrime.

---

[6] Irmanjaya Thaher, *Politik Hukum Pembubaran Organisasi Kemasyarakatan Dalam Perspektif Hak Asasi Manusia*, ed. Daelami Ahmad (Bandung: CV Widina Media Utama, 2023), www.freepik.com.
[7] Dedy Hariyadi et al., *Buku Panduan Dasar Forensik Digital* (Baskara Media, 2020).

HASIL DAN PEMBAHASAN

Bentuk kekosongan hukum dalam pengaturan digital forensik di Indonesia dalam konteks penegakan hukum siber, jika dibandingkan dengan regulasi digital forensik di Amerika Serikat dan Uni Eropa

Kekosongan hukum dalam pengaturan digital forensik di Indonesia mencerminkan belum optimalnya negara dalam memenuhi kewajiban konstitusional sebagai rechtsstaat (negara hukum) sebagaimana tertuang dalam Pasal 1 ayat (3) UUD NRI 1945. Indonesia belum memiliki undang-undang khusus yang secara komprehensif mengatur tata cara pemerolehan, pengamanan, analisis, dan validasi bukti digital dalam proses penegakan hukum siber. Sebagian besar penanganan bukti elektronik masih bergantung pada ketentuan umum dalam UU ITE dan KUHAP, yang belum merespons tantangan teknis digital forensik modern. Hal ini memperlihatkan adanya kekosongan norma baik secara substantif maupun prosedural. Dalam konteks Hukum Tata Negara, kondisi ini mengancam pemenuhan hak konstitusional warga negara atas kepastian hukum (Pasal 28D ayat (1) UUD 1945) dan perlindungan terhadap hak privasi serta *due process of law*.

Sebagai perbandingan, Amerika Serikat telah menerapkan Federal Rules of Evidence 902 dan Daubert Standard yang mengatur tentang keabsahan bukti elektronik serta uji ilmiah terhadap bukti digital. Di samping itu, NIST SP 800-61 dan NIST SP 800-86 menjadi pedoman standar teknis yang digunakan secara nasional dalam praktik digital forensik.

Sementara itu, Uni Eropa mengatur digital forensik secara terpadu dengan pendekatan perlindungan data melalui General Data Protection Regulation (GDPR), ISO/IEC 27037, serta koordinasi antarnegara oleh ENISA dan Europol. Standar teknis dan prinsip hukum materiil di Uni Eropa memastikan bahwa setiap proses perolehan dan penyimpanan bukti elektronik sesuai dengan prinsip legalitas dan proporsionalitas.

Perbandingan ini menunjukkan bahwa Indonesia masih berada pada tahap normatif awal dalam mengatur digital forensik. Tidak adanya pengaturan yang setara dengan NIST atau GDPR mengakibatkan aparat penegak hukum Indonesia tidak memiliki pedoman yang pasti, dan kondisi ini membuka ruang ketidakpastian hukum dalam proses pembuktian. Dalam perspektif Hukum Tata Negara, kekosongan hukum ini berpotensi menjadi bentuk pelanggaran kewajiban negara untuk menjamin perlindungan hak- hak konstitusional warganya, termasuk hak atas keadilan dan proses hukum yang adil. Oleh karena itu, perlu adanya pembentukan regulasi nasional digital forensik yang memuat standar teknis, mekanisme akuntabilitas, serta jaminan konstitusional dalam penanganan bukti elektronik.

Strategi aparat penegak hukum di Indonesia dalam menjaga kredibilitas bukti elektronik dalam menghadapi teknik anti-digital forensik seperti data wiping, ditinjau dari tanggung jawab konstitusional negara menurut perspektif Hukum Tata Negara

Dalam menghadapi tantangan kejahatan siber, aparat penegak hukum di Indonesia menghadapi hambatan tambahan berupa teknik anti-digital forensik, seperti data wiping, yang bertujuan untuk menghapus jejak digital dan menghilangkan bukti elektronik. Strategi yang diterapkan oleh aparat penegak hukum untuk menjaga kredibilitas bukti elektronik dalam konteks ini masih berlandaskan pada regulasi yang berlaku, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta mengacu pada standar internasional, yaitu ISO/IEC 27037:2019 tentang *guidelines for identification, collection, acquisition and preservation of digital evidence*.

Salah satu strategi utama adalah penerapan prinsip first responder yang menjadi ujung tombak dalam tahap awal penanganan barang bukti elektronik. Petugas yang pertama kali menangani lokasi kejadian atau perangkat digital harus mampu mengidentifikasi potensi ancaman terhadap bukti, termasuk risiko terhapusnya data akibat teknik anti-forensik. Dalam praktiknya, mereka dituntut untuk bertindak cepat, hati-hati, dan sesuai dengan pedoman yang berlaku, demi mencegah kerusakan atau kontaminasi data digital.

Untuk memastikan integritas dan kredibilitas barang bukti elektronik, aparat penegak hukum juga menerapkan konsep chain of custody (rantai pengawasan barang bukti). Chain of custody merupakan serangkaian proses dokumentasi dan pelacakan terhadap siapa saja yang menangani barang bukti, kapan, di mana, dan untuk tujuan apa. Setiap perpindahan atau tindakan terhadap barang bukti dicatat secara sistematis agar tidak menimbulkan keraguan di kemudian hari, khususnya saat proses pembuktian di pengadilan.

Dengan menggunakan pendekatan berbasis ISO/IEC 27037 dan memperkuat implementasi *chain of custody*, aparat penegak hukum di Indonesia berupaya meningkatkan akuntabilitas dan profesionalisme dalam menghadapi kejahatan siber yang semakin kompleks. Meskipun secara regulatif masih bergantung pada UU ITE yang bersifat umum, penggunaan standar internasional menjadi langkah strategis dalam mengisi kekosongan aturan teknis dan meningkatkan kepercayaan terhadap keabsahan barang bukti elektronik.

Strategi yang dapat dilakukan oleh aparat penegak hukum di Indonesia dalam menjaga kredibilitas bukti elektronik dalam menghadapi teknik anti-digital forensik seperti data wiping antara lain:

1. Landasan Regulasi

Penegakan hukum atas bukti elektronik di Indonesia telah mengalami kemajuan penting melalui pemberlakuan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diamandemen dengan Undang-Undang Nomor 19 Tahun 2016 dan terbaru dengan Undang-Undang Nomor 1 Tahun 2024. Undang-undang ini menegaskan legitimasi informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah, sebagaimana dinyatakan dalam Pasal 5 ayat (1) yang menyatakan bahwa "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah". Pasal ini mengukuhkan peran bukti elektronik sebagai kelanjutan dari bentuk alat bukti tradisional dalam sistem hukum Indonesia, khususnya dalam menghadapi kejahatan siber, penipuan finansial, pelanggaran konten digital, dan pelanggaran data. Namun demikian, kerangka regulasi ini masih memiliki kekurangan teknis yang signifikan. Tidak terdapat pedoman teknis yang komprehensif mengenai prosedur analisis forensik digital, seperti metode standar pengumpulan data, pelestarian, autentikasi, dan interpretasi bukti digital. Selain itu, undang-undang ini belum menjelaskan secara rinci siapa yang berwenang melakukan investigasi forensik digital serta mekanisme untuk menjaga kredibilitas dan keabsahan bukti melalui audit independen atau jaminan mutu.[8] Kekosongan ini berpotensi menimbulkan sengketa terkait legalitas dan keandalan bukti elektronik, terutama dalam kasus dengan data yang kompleks dan lintas yurisdiksi. Menghadapi tantangan tersebut, aparat penegak hukum di Indonesia mengadopsi berbagai strategi untuk menjaga kredibilitas bukti elektronik, terutama dalam menghadapi teknik anti-digital forensik seperti data wiping yang bertujuan menghapus jejak digital. Salah satu strategi utama adalah penerapan standar internasional ISO/IEC 27037:2012 sebagai pedoman teknis dalam identifikasi, pengumpulan, akuisisi, dan pelestarian bukti digital. Selain itu, *konsep chain of custody* diterapkan secara ketat untuk memastikan integritas bukti dari TKP hingga persidangan. Petugas first responder juga dilatih untuk bertindak cepat dan sistematis dalam mengamankan perangkat dan mencegah hilangnya data akibat teknik penghapusan digital yang dilakukan pelaku kejahatan. Dengan demikian, meskipun secara regulatif Indonesia telah mengakui legalitas bukti digital melalui UU ITE, kekurangan standar teknis dan pedoman operasional masih menjadi tantangan utama. Oleh karena itu, penguatan kerangka teknis dan peningkatan kapasitas aparat penegak hukum sangat diperlukan untuk menjamin bahwa bukti elektronik dapat diterima secara kredibel dan efektif dalam proses peradilan.

2. Penerapan ISO/IEC 27037:2012

Menyediakan panduan teknis untuk identifikasi, pengumpulan, akuisisi, dan pelestarian bukti digital, Menjamin bahwa barang bukti tidak rusak, diubah, atau kehilangan nilai hukum.

3. Tugas dan Tanggung Jawab First Responder

Mengamankan perangkat digital dan lingkungan sekitar TKP, Mencegah proses data wiping atau remote deletion yang bisa dilakukan pelaku. Mencatat semua tindakan awal secara sistematis.

4. Penerapan Chain of Custody

Mencatat seluruh tahapan penanganan barang bukti elektronik sejak awal, menyediakan dokumen pendukung untuk validitas dan integritas bukti, Menjadi alat kontrol terhadap penyalahgunaan atau manipulasi barang bukti.

5. Penggunaan Teknologi Pendukung

Write-blocker digunakan agar perangkat penyimpanan tidak dapat ditulis ulang saat dianalisis, Imaging tools untuk membuat salinan forensik *(forensic image)* dari perangkat yang disita.

---

[8] Handar Subhandi Bakhtiar et al., "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia," *Egyptian Journal of Forensic Sciences* 15, no. 1 (May 29, 2025): 39, https://doi.org/10.1186/s41935-025-00456-y.

6. Pelatihan dan Sertifikasi Aparat Penegak Hukum

Meningkatkan kapasitas teknis penyidik dalam menghadapi teknik anti-digital forensic, Memastikan setiap personel memahami ISO 27037 dan praktik digital forensik global.

Dalam perspektif Hukum Tata Negara, strategi di atas merupakan bagian dari pelaksanaan tanggung jawab konstitusional negara untuk menjamin hak atas keadilan, kepastian hukum, dan perlindungan privasi sebagaimana diatur dalam Pasal 28D dan 28G UUD NRI 1945. Negara wajib membentuk dan memperkuat kerangka hukum teknis sebagai wujud nyata prinsip negara hukum (*rechtstaat*) yang adaptif terhadap perkembangan teknologi.

KESIMPULAN

Kekosongan hukum dalam pengaturan digital forensik di Indonesia masih terjadi, baik secara substantif maupun prosedural. Hal ini ditunjukkan dengan belum adanya regulasi nasional yang secara khusus dan komprehensif mengatur mengenai tata cara identifikasi, pengumpulan, pelestarian, dan pengujian bukti digital dalam sistem peradilan pidana. Jika dibandingkan dengan Amerika Serikat dan Uni Eropa, Indonesia tertinggal dalam hal pengaturan teknis maupun jaminan konstitusional terhadap perlindungan hak atas bukti elektronik.

Strategi yang dilakukan oleh aparat penegak hukum dalam menghadapi teknik anti-digital forensik seperti data wiping mencakup penerapan prinsip first responder, chain of custody, penggunaan standar ISO/IEC 27037, dan pelatihan teknis aparat. Namun, seluruh strategi tersebut belum didukung oleh kerangka hukum nasional yang baku, sehingga berpotensi menimbulkan keraguan terhadap keabsahan pembuktian dan dapat bertentangan dengan prinsip *due process of law*.

Dalam perspektif Hukum Tata Negara, negara Indonesia sebagai negara hukum berdasarkan Pasal 1 ayat (3) UUD NRI 1945 memiliki tanggung jawab konstitusional untuk menyusun regulasi digital forensik yang responsif terhadap tantangan teknologi dan menjamin kepastian hukum. Ketiadaan pengaturan ini dapat dianggap sebagai bentuk kelalaian negara dalam memenuhi jaminan konstitusional terhadap keadilan, hak atas informasi, dan perlindungan privasi.

DAFTAR PUSTAKA

Army, Eddy. *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika, 2020.

Bakhtiar, Handar Subhandi, Amir Ilyas, Abdul Kholiq, and Handina Sulastrina Bakhtiar. "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia." *Egyptian Journal of Forensic Sciences* 15, no. 1 (May 29, 2025): 39. https://doi.org/10.1186/s41935-025-00456-y.

Hariyadi, Dedy, Bambang Sadewo, Kholis Munajat, Dimas Pratama, Nur Rosid Wakhid Wahyudi, Velisia Amanda Khafid, Bagas Saktiawan Prasojo, Benyamin Armanto Ngadu Djawa, Ahmad Gofiansah, and Achmad Alief. *Buku Panduan Dasar Forensik Digital*. Baskara Media, 2020.

Pansariadi, Rafi Septia Budianto, and Noenik Soekorini. "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya." *Binamulia Hukum* 12, no. 2 (December 20, 2023): 287–98. https://doi.org/10.37893/jbh.v12i2.605.

Rachmie, Synthiana. "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website." *Litigasi* 21, no. 1 (2020): 104–27.

Sitorus, Sahat Parulian, Sartika Riama Sidauruk Sakinah, Yudi Alamsyah, Ansell Sun, and Ali Akbar Ritonga. "Digital Cyber Forensics." *JURNAL ARJUNA* 1, no. 1 (2023): 7–10.

Thaher, Irmanjaya. *Politik Hukum Pembubaran Organisasi Kemasyarakatan Dalam Perspektif Hak Asasi Manusia*. Edited by Daelami Ahmad. Bandung: CV Widina Media Utama, 2023. www.freepik.com.

Wibowo, Agus. *Digital Forensik*. Semarang: Penerbit Yayasan Prima Agus Teknik, 2023.