KAMPUS AKADEMIK PUBLISING
Jurnal Akademik Pengabdian Masyarakat
Vol.4, No.1 Januari 2026
e-ISSN: 3030-8631; p-ISSN: 3030-864X, Hal 162-169
DOI: https://doi.org/10.61722/japm.v4i1.7666

Peran Audit dan Hukum dalam Keamanan Informasi, Mengenalkan Aspek Hukum, Aturan, dan Bukti Digital yang Berlaku di Indonesia.

Anisa Sofiana
Universitas Islam Negeri Sulthan Thaha Saifuddin
Adam Tabrani
Universitas Islam Negeri Sulthan Thaha Saifuddin
Nabila Andriani
Universitas Islam Negeri Sulthan Thaha Saifuddin
Ade Novia Maulana
Universitas Islam Negeri Sulthan Thaha Saifuddin
Jl. Arif Rahman Hakim No. 111, Simpang IV Sipin, Kec. Telanaipura, Kota Jambi, Jambi 36124
Korespondensi penulis: andrianinblandriani@gmail.com

Abstrak. *This study aims to analyze the importance of identity management and strong This research aims to analyze the convergence between information systems auditing and the cyber security legal framework in Indonesia. Amidst the escalation of cyber threats targeting national critical infrastructure, information security is no longer merely a technical issue but a binding legal obligation. This study highlights how the audit process functions as a compliance validation mechanism against positive regulations in Indonesia, specifically the Personal Data Protection Law (UU PDP) and the Electronic Information and Transactions Law (UU ITE). The research method used is descriptive qualitative with a juridical-normative approach. The results of this study are expected to map out procedures for handling digital evidence that are valid in the eyes of Indonesian law and formulate audit standards capable of mitigating legal risks for organizations. Initial findings suggest that the integration of standardized audit logs (ISO 27001) is crucial in digital forensic evidence in court*
Keywords: *Information Security, System Audit, Digital Evidence, UU ITE, UU PDP, Digital Forensics.*

Abstrak. Penelitian ini bertujuan untuk menganalisis konvergensi antara audit sistem informasi dan kerangka hukum keamanan siber di Indonesia. Di tengah eskalasi ancaman siber yang menargetkan infrastruktur kritis nasional, keamanan informasi tidak lagi sekadar isu teknis, melainkan kewajiban hukum yang mengikat. Studi ini menyoroti bagaimana proses audit berfungsi sebagai mekanisme validasi kepatuhan terhadap regulasi positif di Indonesia, khususnya Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Metode penelitian yang digunakan adalah kualitatif deskriptif dengan pendekatan yuridis-normatif. Hasil penelitian ini diharapkan dapat memetakan prosedur penanganan bukti digital (digital evidence) yang sah di mata hukum Indonesia serta merumuskan standar audit yang mampu memitigasi risiko hukum bagi organisasi. Temuan awal menunjukkan bahwa integrasi log audit yang terstandarisasi (ISO 27001) sangat krusial dalam pembuktian forensik digital di pengadilan
Kata Kunci: *Keamanan Informasi, Audit Sistem, Bukti Digital, UU ITE, UU PDP, Forensik Digital.*

PENDAHULUAN

Transformasi digital di Indonesia telah menciptakan ekosistem siber yang kompleks, di mana data menjadi komoditas strategis sekaligus titik kerentanan utama. Fenomena kebocoran data dan intrusi siber yang terjadi pada berbagai sektor publik maupun privat di Indonesia menunjukkan adanya kesenjangan antara penerapan teknologi pengamanan dan kepatuhan terhadap regulasi. Dalam konteks ini, keamanan informasi tidak bisa lagi dipandang semata-mata sebagai upaya preventif teknis (seperti penggunaan *firewall* atau enkripsi), namun harus diposisikan sebagai objek audit yang memiliki implikasi hukum serius.

Received November 28, 2025; Revised Desember 15, 2025; Januari 01, 2026
* Nabila Andriani, andrianinblandriani@gmail.com

Negara telah merespons dinamika ini melalui instrumen hukum yang ketat, diantaranya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kedua regulasi ini menuntut penyelenggara sistem elektronik (PSE) untuk menjamin keandalan sistem dan keamanan data. Kegagalan dalam membuktikan keandalan sistem saat terjadi insiden siber dapat berujung pada sanksi administratif hingga pidana.

Disinilah peran audit keamanan informasi menjadi krusial. Audit tidak hanya berfungsi untuk menemukan celah keamanan (*vulnerability assessment*), tetapi juga menghasilkan *audit trail* atau jejak audit. Dalam perspektif hukum, jejak audit ini berpotensi menjadi bukti digital yang sah apabila dikelola sesuai dengan prinsip *Chain of Custody*. Namun, di lapangan, seringkali ditemukan ketidaksinkronan antara standar audit teknis yang dilakukan oleh profesional IT dengan persyaratan alat bukti yang diminta oleh aparat penegak hukum di Indonesia.

Oleh karena itu, penelitian ini hadir untuk menjembatani perspektif teknis dan yuridis tersebut. Penulis, sebagai peneliti, merasa perlu untuk menguraikan bagaimana mekanisme audit dapat memperkuat posisi hukum suatu organisasi dan bagaimana aspek regulasi Indonesia mengatur validitas bukti digital yang dihasilkan dari proses pengamanan informasi

KAJIAN TEORITIS

Sejarah Keamanan Informasi

Sejarah keamanan informasi telah berevolusi secara dinamis dari sekadar pengamanan fisik perangkat keras pada era awal komputasi mainframe, menjadi suatu disiplin ilmu kompleks yang kini berfokus pada perlindungan aset data di tengah interkonektivitas jaringan global yang tanpa batas. Transformasi paradigma ini menuntut organisasi untuk memandang keamanan siber bukan lagi sebagai isu teknis semata, melainkan sebagai kewajiban tata kelola perusahaan yang krusial untuk memitigasi risiko serangan digital yang semakin canggih dan persisten. Oleh karena itu, strategi pertahanan informasi saat ini harus mengintegrasikan aspek teknologi dan kebijakan manajemen secara utuh, sehingga perlindungan informasi kini menjadi fondasi utama dalam menjaga stabilitas infrastruktur kritis dari ancaman eksternal.

Definisi keamanan informasi dalam konteks terkini dipahami sebagai proses manajemen risiko strategis yang dirancang untuk menjamin kerahasiaan, integritas, dan ketersediaan seluruh aset informasi agar terhindar dari akses ilegal maupun modifikasi yang tidak sah oleh pihak ketiga. Konsep ini menekankan bahwa penerapan teknologi keamanan harus berjalan beriringan dengan kepatuhan terhadap regulasi hukum yang berlaku di Indonesia, di mana setiap mekanisme kontrol yang diterapkan wajib menghasilkan bukti audit yang valid guna memastikan akuntabilitas sistem serta menjamin keberlangsungan operasional organisasi dalam menghadapi berbagai potensi insiden keamanan

Audit Sistem Informasi Berbasis Risiko

Audit sistem informasi didefinisikan sebagai suatu proses sistematis dan terstruktur dalam mengumpulkan serta mengevaluasi bukti-bukti objektif untuk memverifikasi apakah sistem komputer suatu organisasi mampu mengamankan aset kritis secara optimal

. Proses ini tidak hanya bertujuan untuk memelihara integritas data agar tetap akurat dan andal, tetapi juga memastikan bahwa penggunaan teknologi informasi dapat mendukung pencapaian tujuan organisasi secara efektif serta efisien. Dalam pelaksanaannya, audit sistem menuntut adanya pemeriksaan menyeluruh terhadap tata kelola teknologi, infrastruktur jaringan, hingga prosedur operasional guna mendeteksi adanya penyimpangan yang berpotensi merugikan kinerja keseluruhan sistem.

Berbeda dengan audit finansial konvensional, pendekatan yang diterapkan dalam penelitian ini difokuskan pada Audit Berbasis Risiko (*Risk-Based Audit*) yang dinilai lebih adaptif terhadap dinamika ancaman siber saat ini. Metode ini memprioritaskan alokasi sumber daya pemeriksaan pada area-area sistem yang memiliki profil risiko kegagalan tertinggi atau yang berpotensi menimbulkan dampak hukum signifikan bagi keberlangsungan perusahaan. Dengan memetakan kerentanan berdasarkan tingkat keparahan risiko, auditor dapat memberikan rekomendasi yang lebih tepat sasaran untuk memitigasi celah keamanan yang krusial, sehingga organisasi tidak hanya sekadar memenuhi standar administrasi, tetapi benar-benar terlindungi dari ancaman nyata yang dapat melumpuhkan operasional

Ancaman Terhadap Identitas Digital

penelitian ini secara spesifik mengadopsi acuan standar internasional ISO/IEC 27001 mengenai Sistem Manajemen Keamanan Informasi (SMKI) sebagai landasan utama evaluasi kontrol keamanan. Kerangka kerja *best practice* yang telah diakui secara global karena pendekatannya yang komprehensif dalam mengelola risiko informasi, serta secara aktif dijadikan rujukan primer oleh Badan Siber dan Sandi Negara (BSSN) menetapkan parameter keamanan siber nasional di Indonesia.

Penerapan standar ini tidak hanya berfungsi untuk menstandarisasi prosedur teknis semata, melainkan juga memastikan bahwa tata kelola perlindungan data yang diterapkan organisasi telah memenuhi kualifikasi kepatuhan yang ketat, terukur, dan selaras dengan tuntutan keamanan modern yang bersifat dinamis untuk menjaga kerahasiaan data vital

Tinjauan Yuridis: Rezim Hukum Siber di Indonesia

Indonesia secara fundamental menganut sistem hukum tertulis (*Civil Law*), yang meniscayakan bahwa seluruh standar validitas keamanan informasi dan tata kelola sistem elektronik harus senantiasa merujuk pada regulasi positif yang berlaku secara hierarkis. Dalam ekosistem digital yang berkembang pesat saat ini, kepatuhan terhadap peraturan perundang-undangan bukan hanya menjadi kewajiban administratif, melainkan prasyarat mutlak untuk menjamin legitimasi operasional serta perlindungan hak subjek data pengguna. Oleh karena itu, analisis yuridis dalam perancangan ini tidak dapat dilepaskan dari ketentuan formal yang mengikat guna memastikan akuntabilitas hukum yang kuat

Bukti Digital (*Digital Evidence*)

Bukti digital didefinisikan sebagai segala entitas informasi yang disimpan atau ditransmisikan dalam format biner dan memiliki nilai probatif yang dapat diandalkan dalam persidangan. Secara fundamental, karakteristik bukti ini berbeda dengan bukti fisik konvensional karena sifatnya yang *Latent* (tersembunyi) sehingga memerlukan bantuan komputasi untuk diakses, *Fragile* (mudah rusak) karena sangat rentan terhadap alterasi data, serta *Volatile* (mudah hilang) ketika catu daya perangkat diputus. Kompleksitas karakteristik unik tersebut menuntut

penerapan metode forensik yang ketat guna menjaga orisinalitas data sebelum dihadirkan sebagai alat bukti hukum yang sah

Forensik Digital dan Chain of Custody

Forensik digital merupakan disiplin ilmu yang mengintegrasikan prinsip ilmu komputer dan teknologi informasi untuk kepentingan pembuktian hukum melalui identifikasi, pelestarian, dan analisis data digital. Dalam konteks audit keamanan sistem informasi, metode forensik tidak hanya berfungsi untuk menemukan kerentanan, tetapi juga berperan vital dalam merekonstruksi insiden keamanan secara komprehensif guna mengungkap kronologi serangan. Penerapan standar forensik yang ketat memastikan bahwa setiap temuan teknis yang dihasilkan memiliki landasan ilmiah yang kuat sehingga dapat dipertanggungjawabkan keabsahannya ketika diajukan sebagai fakta persidangan maupun laporan audit resmi

Manajemen Identitas Berbasis Cloud

Manajemen Identitas Berbasis Cloud (IDaaS) adalah model penyampaian layanan yang menyediakan solusi manajemen identitas melalui cloud. IDaaS menawarkan beberapa keuntungan, termasuk:

A. Skalabilitas: Mampu menangani peningkatan jumlah pengguna dan aplikasi.
B. Fleksibilitas: Memungkinkan organisasi untuk dengan mudah mengintegrasikan solusi manajemen identitas dengan aplikasi cloud dan on-premise.
C. Efisiensi Biaya: Mengurangi biaya modal dan operasional yang terkait dengan pengelolaan infrastruktur manajemen identitas.
D. Keamanan: Menyediakan fitur keamanan canggih seperti MFA dan deteksi ancaman berbasis AI

Peran Auditor dan Ahli Forensik dalam Litigasi

Dalam ekosistem hukum di Indonesia, peran seorang auditor sistem informasi maupun ahli forensik digital memegang posisi strategis yang seringkali beririsan langsung dengan fungsi Saksi Ahli (Expert Witness) di dalam proses peradilan pidana maupun perdata. Legitimasi peran profesi ini diperkuat secara yuridis oleh ketentuan dalam Pasal 186 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang secara tegas menempatkan keterangan ahli sebagai salah satu alat bukti yang sah dan memiliki kekuatan pembuktian mandiri. Kehadiran mereka di muka persidangan bukan sekadar sebagai teknisi pelapor data, melainkan sebagai instrumen vital yang membantu aparat penegak hukum dalam membedah anatomi kasus kejahatan siber yang memiliki karakteristik pembuktian yang rumit, abstrak, dan tidak kasat mata secara fisik

METODE PENELITIAN

Dalam konteks penelitian ini, proses pengumpulan data dilakukan dengan memanfaatkan sumber-sumber yang tersedia secara luas di platform daring seperti Google dan Google Scholar. Pendekatan ini memungkinkan peneliti untuk mengakses berbagai macam informasi yang relevan dengan topik manajemen identitas dan kata sandi yang kuat, termasuk artikel ilmiah, laporan industri, studi kasus, dan publikasi lainnya. Pencarian dilakukan dengan menggunakan kata kunci yang relevan dan kombinasi kata kunci, serta memanfaatkan fitur pencarian lanjutan yang tersedia di Google dan Google Scholar untuk mempersempit hasil pencarian dan memastikan relevansi data.

Setelah data dikumpulkan, langkah selanjutnya adalah melakukan evaluasi kritis terhadap kualitas dan kredibilitas sumber. Hal ini melibatkan peninjauan terhadap reputasi penulis atau penerbit, konsistensi informasi dengan sumber lain. Hanya sumber-sumber yang dianggap relevan yang akan dimasukkan dalam analisis. Selain itu, peneliti juga berusaha untuk mengidentifikasi potensial dalam sumber-sumber yang digunakan dan mempertimbangkan untuk memastikan representasi yang seimbang dari berbagai sudut pandang.

Proses pengumpulan data ini dilakukan secara sistematis dan transparan, dengan mencatat semua langkah yang diambil dan keputusan yang dibuat. Hal ini memungkinkan peneliti lain untuk mereplikasi proses pengumpulan data dan memverifikasi temuan penelitian. Meskipun penelitian ini bergantung pada sumber-sumber, peneliti tetap berupaya untuk memastikan bahwa data yang digunakan akurat, relevan, dan representatif dari topik yang sedang diteliti. Dengan demikian, diharapkan penelitian ini dapat memberikan wawasan yang berharga tentang pentingnya manajemen identitas dan kata sandi yang kuat, serta memberikan panduan praktis untuk individu dan organisasi dalam melindungi aset digital mereka

HASIL PENELITIAN DAN PEMBAHASAN

1. Strategis Manajemen Identitas

Hasil analisis mendalam terhadap tata kelola keamanan informasi pada objek penelitian, ditemukan adanya kesenjangan (*gap*) yang sangat signifikan antara penerapan standar keamanan teknis dengan pemenuhan kepatuhan hukum (*legal compliance*). Fenomena yang umum terjadi di lapangan adalah banyak organisasi di Indonesia yang memfokuskan sumber daya mereka hanya pada pengamanan perimeter jaringan seperti instalasi *firewall* semata, namun cenderung abai terhadap amanat krusial Pasal 15 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal ini secara tegas mewajibkan setiap Penyelenggara Sistem Elektronik (PSE) untuk menyelenggarakan sistemnya secara andal, aman, dan bertanggung jawab agar beroperasi sebagaimana mestinya.

Hasil studi lebih lanjut menunjukkan fakta bahwa sebuah sistem informasi yang tidak dilengkapi dengan kebijakan retensi data (*data retention policy*) yang terstruktur serta prosedur enkripsi yang standar, secara otomatis menempatkan organisasi tersebut dalam posisi yang sangat rentan di mata hukum. Absennya mekanisme perlindungan data yang baku membuat organisasi kesulitan membuktikan integritas sistemnya saat diaudit. Hal ini menjadi titik lemah fatal karena keamanan data bukan hanya soal mencegah akses ilegal, tetapi juga tentang bagaimana data dikelola dan disimpan sesuai standar privasi. Tanpa protokol ini, organisasi dianggap gagal melakukan langkah preventif yang memadai (*due care*) dalam melindungi aset informasi yang dikelolanya.

Dalam perspektif sistem hukum *Civil Law* yang dianut oleh negara Indonesia, ketiadaan kepatuhan terhadap standar regulasi ini bukan lagi dipandang sekadar isu administratif biasa, melainkan dapat dikategorikan sebagai bentuk kelalaian serius (*negligence*). Kelalaian tata kelola ini memiliki konsekuensi pertanggungjawaban hukum yang berat, baik dalam ranah pidana maupun perdata, terutama apabila terbukti terjadi insiden kebocoran data yang merugikan subjek data. Oleh karena itu, paradigma audit keamanan modern tidak boleh lagi hanya berhenti pada temuan celah teknis atau *vulnerability assessment* semata, melainkan harus diperluas mencakup audit kepatuhan regulasi (*compliance audit*) guna memastikan operasional sistem sepenuhnya selaras dengan koridor hukum positif yang berlaku

2. Arsitektur Kata Sandi yang Kokoh

Dalam pembahasan mendalam mengenai bukti digital, penelitian ini secara khusus menyoroti kompleksitas karakteristik data elektronik yang unik, yaitu bersifat *latent* (tidak kasat mata), *fragile* (sangat mudah rusak), dan *volatile* (mudah berubah atau hilang). Sifat alami ini menuntut perlakuan teknis yang sangat hati-hati karena kesalahan prosedur sekecil apa pun dapat merusak orisinalitas data. Agar temuan dari hasil audit keamanan sistem dapat bertransformasi menjadi alat bukti yang sah dan meyakinkan di pengadilan Indonesia, seluruh bukti tersebut wajib lolos uji validasi dua lapis yang ketat.

Lapis pertama adalah validasi materiil, di mana integritas data harus dijamin mutlak melalui teknologi *hashing* untuk memastikan bahwa tidak ada manipulasi atau perubahan data pasca-insiden. Selanjutnya, lapis kedua adalah validasi formil yang mensyaratkan bahwa prosedur perolehan bukti harus sepenuhnya sah menurut hukum acara pidana (*due process of law*) tanpa melanggar ketentuan perundang-undangan. Apabila salah satu dari unsur validitas ini cacat, misalnya perolehan bukti dilakukan secara ilegal, maka bukti digital tersebut berisiko besar dikesampingkan oleh hakim dan kehilangan nilai pembuktiannya di meja hijau.

Pertama, Validasi Materiil: Bukti harus terjamin integritasnya. Temuan audit berupa *log file* atau rekaman lalu lintas data wajib disertai dengan nilai *hash* (seperti SHA-256) untuk membuktikan bahwa data tersebut otentik dan tidak mengalami manipulasi (*tampering*) pasca-insiden.

Kedua, Validasi Formil: Prosedur perolehan bukti harus sah secara hukum. Hasil pembahasan menegaskan bahwa bukti yang didapat melalui cara-cara ilegal (misalnya intersepsi tanpa hak) akan gugur demi hukum karena melanggar prinsip *due process of law*, meskipun bukti tersebut secara teknis relevan dengan kasus yang sedang ditangani

3. Chain of Custody dalam Prosedur Audit

Hasil penelitian ini secara tegas menempatkan *Chain of Custody* (Rantai Pengawasan) sebagai instrumen paling vital yang berfungsi menjembatani proses teknis audit dengan proses pembuktian hukum. Berdasarkan analisis kasus, ditemukan fakta bahwa kegagalan terbesar dalam litigasi siber seringkali bukan disebabkan oleh ketiadaan bukti, melainkan karena terputusnya rantai dokumentasi barang bukti tersebut. Ketiadaan jejak audit yang utuh menyebabkan keraguan hakim terhadap validitas asal-usul data yang disajikan, sehingga bukti tersebut kehilangan legitimasi formalnya dalam persidangan.

Dalam simulasi penanganan insiden, prosedur pencatatan kronologis yang mendetail mulai dari identitas personel yang mengakuisisi data, waktu spesifik akuisisi dilakukan, hingga lokasi penyimpanan bukti terbukti menjadi benteng pertahanan utama. Dokumentasi yang presisi ini sangat krusial untuk mematahkan argumen penyangkalan (*repudiation*) yang sering diajukan oleh pihak lawan. Tanpa catatan logistik yang akurat ini, integritas bukti menjadi sangat mudah untuk diserang dan dianggap tidak kredibel.

Tanpa penerapan *Chain of Custody* yang disiplin dan ketat, metadata yang melekat pada bukti digital dapat dianggap telah terkontaminasi oleh intervensi yang tidak sah,

sehingga nilai pembuktiannya (*probative value*) di hadapan Majelis Hakim menjadi lemah atau bahkan ditolak sepenuhnya. Kondisi ini menegaskan bahwa penerapan standar internasional ISO 27037 tentang pedoman identifikasi, pengumpulan, akuisisi, dan pelestarian bukti digital bukan lagi sekadar opsi, melainkan menjadi standar imperatif yang harus diadopsi secara penuh dalam prosedur audit keamanan di Indonesia demi menjamin kepastian hukum

4. Peran Auditor Menjadi Saksi Ahli (*Expert Witness*)

Peran profesi auditor dalam ranah litigasi. Dalam ekosistem hukum yang berlaku di Indonesia, laporan hasil audit keamanan informasi berfungsi fundamental sebagai landasan utama bagi auditor untuk memberikan keterangan sebagai Ahli di muka persidangan. Hal ini memiliki legitimasi yuridis yang kuat dan diakui sebagai alat bukti sah sebagaimana diatur secara tegas dalam ketentuan Pasal 186 Undang-Undang Hukum Acara Pidana (KUHAP).

Peran seorang auditor kini tidak lagi sebatas menemukan *bug* atau *vulnerability* teknis semata, melainkan dituntut harus mampu menerjemahkan berbagai terminologi teknis yang rumit seperti *SQL Injection*, *DDoS*, atau *Malware Analysis*. Kemampuan komunikasi ini vital untuk mengubah data biner menjadi narasi kausalitas yang logis agar dapat dipahami dengan jelas oleh aparat penegak hukum yang umumnya awam terhadap teknologi. Tanpa simplifikasi yang akurat dan dapat dipertanggungjawabkan ini, fakta-fakta digital akan sulit diterima sebagai kebenaran materil oleh hakim dalam memutus perkara.

Analisis ini menunjukkan bahwa kualitas dan kejelasan laporan audit sangat menentukan konstruksi hukum sebuah kasus siber, yakni untuk membedakan secara presisi apakah insiden tersebut murni serangan siber dari pihak luar (*cyber attack*) atau merupakan akibat fatal dari kelalaian tata kelola internal (*internal fraud/negligence*). Pembedaan kausalitas ini sangat krusial karena menentukan arah pertanggungjawaban pidana yang akan dijatuhkan. Dengan demikian, kompetensi seorang auditor keamanan informasi di Indonesia saat ini harus bersifat hibrida, di mana ia wajib menguasai teknis forensik secara mendalam sekaligus memahami logika pembuktian hukum yang berlaku

KESIMPULAN

Hasil penelitian ini dapat disimpulkan bahwa mengenai Peran Audit dan Hukum dalam Keamanan Informasi: Mengenalkan Aspek Hukum, Aturan, dan Bukti Digital yang Berlaku di Indonesia, dapat disimpulkan bahwa keamanan informasi di Indonesia tidak dapat lagi dipandang sebagai isu teknis yang terpisah, melainkan merupakan kewajiban fundamental yang terintegrasi dengan rezim hukum siber. Penerapan sistem yang andal dan aman wajib didasarkan pada kepatuhan terhadap regulasi positif seperti UU ITE dan UU Perlindungan Data Pribadi. Integritas sistem, mulai dari manajemen identitas dan penggunaan kata sandi yang kuat hingga konfigurasi infrastruktur, secara langsung memengaruhi kekuatan pembuktiannya di pengadilan. Bukti digital yang bersifat *latent* dan *volatile* hanya dapat diterima jika memenuhi syarat materiil (keutuhan data melalui *hashing*) dan syarat formil (perolehan yang sah melalui prosedur legal). Kegagalan terbesar dalam litigasi siber adalah terputusnya *Chain of Custody*, yang meruntuhkan nilai pembuktian. Oleh karena itu, auditor sistem informasi memegang peran strategis sebagai Saksi Ahli, yang bertugas menjembatani kesenjangan antara kompleksitas teknis forensik dengan logika pembuktian hukum, memastikan bahwa temuan teknis dapat dipertanggungjawabkan dalam penegakan hukum siber.

DAFTAR PUSTAKA

Andhitya, R. (2025). ANALISIS KRITIS PENEGAKAN HUKUM KEJAHATAN SIBER DATA. Bandung : Hukum Lex Generali.

Budianto, A. S. (2024). Perluasan dari Alat Bukti Tertulis dalam Perspektif Hukum Acara. Law, Development & Justice Review.

Febrian. (2025). Implikasi Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Fintech. Jakarta: Rechtsnormen Jurnal Komunikasi dan Informasi Hukum.

Handayani, A. (2025). Penegakan Hukum Terhadap Praktik Judi Online di Era Digital:. Banten: Al-Zayn : Jurnal Ilmu Sosial & Hukum.

Hasanah, N. U. (2025). Analisis Keamanan Komunikasi Aplikasi WAVE Mobile Communicator pada Ponsel Hybrid dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037. Yogyakarta.

PUTRI, O. S. (2023). Tinjauan Yuridis Keabsahan dan Kekuatan Peembuktian Tanda Tangan Elektronik (DIGITAL SIGNATURE) Dengan Menggunakan Aplikasi Privy Dalam Perjanjian Berdasarkan KUHPERDATA. Riau.

Qonita, I. T. (2020). Analisis Pengaruh Karakteristik Dewan Pengawas, Syariah, Audit, internal dan Fungsi Kepatuhan Terhadap Kepatuhan Syariah. Yogyakarta.

Ramadhanty, N. (2024). Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber. Journal of Indonesian Management, 1-9.

Rohman. (2024). Sistem Pembuktian dalam Hukum Pidana Indonesia dan. JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin.

Setiawan, A. B. (2014). Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik. Jakarta: Aplikasi Informatika dan Informasi Komunikasi Publik