Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Digital Justice: Tantangan Pembuktian dan Penegakan Hukum Pidana di Era Anonimitas Siber

Bagas Gilang Andika Pratama[1*], Agus Pramono[2], Lailasari Ekaningsih[3]
[1,3]Fakultas Hukum, Universitas Darul Ulum Islamic Centre Sudirman
[2]Fakultas Hukum, Universitas Wisnuwardhana Malang
[*]Email Korespondensi: gilangandika1425@gmail.com

ABSTRAK

Keadilan Digital *(Digital Justice)* merepresentasikan evolusi sistem peradilan pidana dalam menghadapi transformasi masif interaksi sosial ke ranah virtual yang ditandai oleh anonimitas siber dan volatilitas data. Penelitian ini bertujuan untuk menganalisis tantangan kritis dalam pembuktian dan penegakan hukum pidana di era digital dengan fokus pada aspek forensik dan yurisdiksi. Menggunakan metode yuridis normatif dengan pendekatan deskriptif-analitis, studi ini mengeksplorasi bagaimana kerangka hukum tradisional terbebani oleh teknologi yang mengaburkan identitas, seperti VPN, Tor, dan enkripsi. Temuan penelitian menunjukkan bahwa identifikasi pelaku terhambat oleh kesenjangan kompetensi antara aparat penegak hukum dan pelaku kejahatan, sementara akseptabilitas bukti digital sering kali terkompromi oleh ketiadaan protokol standar rantai penjagaan *(chain of custody).* Analisis diperkaya dengan teori *"Code is Law"* dari Lawrence Lessing dan konsep *"Digital Justice"* dari Katsh dan Rabinovich-Einy. Penelitian menyimpulkan bahwa pencapaian keadilan digital memerlukan integrasi multidisiplin antara hukum, teknologi, dan reformasi organisasi untuk memastikan supremasi hukum tetap efektif di lanskap digital tanpa batas.

Kata Kunci: Kejahatan Siber, Bukti Digital, Keadilan Digital, Anonimitas, Yurisdiksi

1. PENDAHULUAN

Transformasi masyarakat menuju era digital telah mengubah lanskap kriminalitas secara fundamental, menciptakan ruang bagi kejahatan yang tidak lagi dibatasi oleh batas-batas geografis tradisional (Farhan et al., 2022). Fenomena kejahatan siber (*cybercrime*) muncul sebagai tantangan global yang signifikan, mengancam keamanan dan stabilitas masyarakat di seluruh dunia (Taher et al., 2025). Kemudahan melakukan kejahatan secara daring, yang didukung oleh infrastruktur internet yang semakin canggih, membuat

pendeteksian, investigasi, dan penuntutan terhadap pelaku menjadi tugas yang sangat kompleks bagi otoritas penegak hukum konvensional (Taher et al., 2025). Di tengah dinamika ini, konsep *Digital Justice* muncul bukan sekadar sebagai istilah teknis, melainkan sebagai tuntutan normatif untuk menyesuaikan sistem peradilan dengan realitas teknologi yang ada.

Penelitian terdahulu telah mengidentifikasi berbagai dimensi dari tantangan ini. Silalahi (2023) menyoroti bahwa kemajuan teknologi informasi telah mengubah lanskap kejahatan, menyebabkan tantangan baru bagi penegakan hukum pidana konvensional. Studi oleh Yustia A., (2010) menekankan bahwa salah satu masalah utama yang dihadapi penegak hukum di Indonesia adalah pembuktian kesalahan terdakwa dalam kasus *cybercrime*, di mana keterangan ahli telematika menjadi alat bukti krusial di bawah payung Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, perkembangan teknologi yang sangat pesat sering kali melampaui kapasitas regulasi yang ada. Firdaus (2024) menggarisbawahi urgensi penanggulangan kejahatan teknologi informasi dalam sistem hukum Indonesia melalui sinkronisasi regulasi dan optimalisasi perangkat pendukung. Lebih lanjut, penelitian oleh Novita et al., (2024) mengungkapkan bahwa meskipun hukum siber di Indonesia telah menunjukkan kemajuan, peraturan yang ada masih belum terintegrasi secara sistemik, menyebabkan kerentanan terhadap kejahatan siber seperti peretasan dan penipuan daring. Terakhir, penelitian oleh Sufian & Eddyono (2024) secara spesifik mengeksplorasi penyelidikan terhadap anonimitas pelaku kejahatan siber di Indonesia, yang menunjukkan bahwa identifikasi pelaku tetap menjadi hambatan teknis dan yuridis yang paling persisten.

Urgensi penelitian ini terletak pada perlunya rekonstruksi pemahaman mengenai penegakan hukum pidana di era anonimitas siber. Terdapat kebutuhan mendesak untuk menjembatani kesenjangan antara hukum formal dengan realitas "kode" digital yang mengatur perilaku di ruang siber. Richard Susskind berpendapat bahwa masa depan

keadilan bukan terletak pada ruang sidang fisik, melainkan pada kemampuan sistem hukum untuk memberikan hasil yang adil melalui teknologi yang dapat diakses dan efisien (Dickson, 2020). Namun, transisi menuju *Digital Justice* ini tidak bebas dari risiko, termasuk potensi pengikisan hak-hak prosedural, bias algoritma, dan eksklusi digital bagi kelompok rentan (Rodríguez-Salcedo et al., 2025).

Orisinalitas atau kebaruan penelitian ini terletak pada integrasi teori-teori hukum asing, seperti *"Code is Law"* dari Lawrence Lessing dan *"Digital Justice"* dari Katsh dan Rabinovich-Einy, ke dalam konteks tantangan penegakan hukum di Indonesia. Penelitian ini juga mengeksplorasi konsep *"Power of Disposal"* sebagai alternatif terhadap model kepemilikan fisik tradisional dalam penyitaan data awan (*cloud storage*) (Karagiannis & Vergidis, 2021). Dengan mengombinasikan perspektif global dan lokal, artikel ini bertujuan untuk memberikan kontribusi teoretis bagi pengembangan hukum pidana siber yang lebih responsif. Signifikansi penelitian ini diharapkan dapat memberikan kerangka kerja bagi pembuat kebijakan dan praktisi hukum dalam menghadapi kompleksitas pembuktian di era digital yang semakin anonim, serta mendorong terciptanya sistem hukum siber yang kuat dan melindungi keamanan nasional (Novita et al., 2024).

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif yang bersifat deskriptif-analitis (Marzuki, 2014). Pendekatan ini difokuskan pada analisis terhadap hukum sebagai norma atau kaidah yang berlaku dalam masyarakat, khususnya terkait dengan regulasi kejahatan siber dan hukum acara pidana digital. Data yang digunakan adalah data sekunder yang diperoleh melalui studi kepustakaan yang ekstensif, mencakup peraturan perundang-undangan, literatur hukum internasional, jurnal ilmiah nasional maupun internasional, serta laporan penelitian terkait.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Analisis dilakukan dengan menggunakan teknik meta-sintesis kualitatif, di mana data dari berbagai studi dikumpulkan untuk mengidentifikasi pola, tantangan, dan solusi dalam penegakan hukum siber (Rakha, 2024). Teori-teori yang digunakan dalam menganalisis topik ini meliputi Modalitas Regulasi Lawrence Lessing, konsep *Digital Justice* dari Katsh dan Rabinovich-Einy, serta prinsip-prinsip forensik digital dari SANS Institute dan ACPO (Karagiannis & Vergidis, 2021). Fokus utama analisis adalah pada sinkronisasi antara regulasi nasional Indonesia (UU ITE dan UU PDP) dengan instrumen hukum internasional seperti Konvensi Budapest dalam menghadapi tantangan anonimitas dan lintas yurisdiksi (Firdaus, 2024). Batasan penelitian ini terletak pada fokusnya terhadap aspek hukum pidana dan prosedur pembuktian, tanpa melakukan pengujian teknis laboratorium forensik secara langsung.

3. HASIL & PEMBAHASAN

Epistemologi Bukti Digital: Validitas, Rantai Penjagaan, dan Tantangan Anonimitas dalam Forensik Modern

Pembuktian dalam hukum pidana siber menghadapi krisis epistemologis karena sifat dasar bukti digital yang secara ontologis berbeda dari bukti fisik konvensional. Bukti digital didefinisikan sebagai informasi atau data yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan sebagai bukti di pengadilan (Karagiannis & Vergidis, 2021). Karakteristik utama bukti ini adalah volatilitasnya yang tinggi, fragilitas, dan kemudahan untuk dimanipulasi tanpa meninggalkan jejak fisik yang kasat mata (Prasad, 2025). Di era anonimitas siber, di mana pelaku menggunakan teknik enkripsi canggih, jaringan *The Onion Router* (Tor), dan *Virtual Private Networks* (VPN) untuk menyembunyikan identitas, beban pembuktian menjadi tantangan eksistensial bagi integritas sistem peradilan pidana (Aini & Lubis, 2024).

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Untuk memastikan validitas bukti digital, literatur internasional merujuk pada standar yang ditetapkan oleh SANS Institute dan ACPO (*Association of Chief Police Officers*). Standar ini berfungsi sebagai jangkar prosedural untuk menjaga agar data digital tidak kehilangan nilai pembuktiannya akibat kesalahan penanganan.

Prinsip (SANS)	**Deskripsi Operasional**	**Relevansi Hukum**
Admissibility	Dikumpulkan melalui prosedur yang sah secara hukum *(due process).*	Menghindari pengesampingan bukti akibat pelanggaran hak konstitusional pelaku.
Authenticity	Bukti harus terhubung secara positif dengan insiden yang diselidiki.	Memastikan data bukan hasil fabrikasi atau "ditanam" secara ilegal.
Completion	Harus menyajikan gambaran utuh, baik bukti yang memberatkan maupun meringankan.	Menjamin keadilan bagi terdakwa dan mencegah bias penuntutan.
Reliability	Metode pengumpulan dan analisis harus teruji secara teknis dan ilmiah.	Menjamin bahwa hasil ekstraksi data akurat dan tidak berubah.
Believability	Disajikan dengan cara yang jelas dan dapat dipahami oleh hakim/juri.	Memastikan interpretasi teknis selaras dengan logika hukum.

Sumber: Diolah dari Karagiannis & Vergidis (2021).

Tantangan terbesar dalam menjaga validitas ini adalah menjaga integritas data selama seluruh siklus hidup investigasi. Prinsip ACPO menegaskan bahwa tidak boleh ada tindakan yang diambil oleh penegak hukum yang dapat mengubah data yang tersimpan di komputer atau media penyimpanan yang nantinya akan diajukan sebagai bukti di pengadilan (Karagiannis & Vergidis, 2021). Namun, dalam realitas forensik, menyalakan perangkat yang disita saja dapat memicu perubahan pada metadata, yang bagi pengacara pembela dapat dijadikan celah untuk meragukan otentisitas bukti tersebut

(Karagiannis & Vergidis, 2021). Oleh karena itu, setiap akses ke data asli harus dilakukan oleh personel yang memiliki kompetensi teknis tinggi dan mampu memberikan kesaksian mengenai implikasi dari tindakan mereka (Karagiannis & Vergidis, 2021).

Rantai Penjagaan (*Chain of Custody* - CoC) muncul sebagai protokol paling kritis dalam dokumentasi bukti digital. CoC bukan sekadar catatan serah terima, melainkan narasi kronologis yang tidak terputus mengenai siapa yang menguasai bukti, kapan, di mana, dan untuk tujuan apa (Badiye et al., 2023). Kegagalan dalam mendokumentasikan setiap transmisi bukti dapat menyebabkan bukti tersebut dinyatakan tidak dapat diterima (*inadmissible*) karena adanya ketidakpastian mengenai integritasnya (Badiye et al., 2023). Studi kontemporer mulai mengeksplorasi penggunaan teknologi *blockchain* untuk menciptakan sistem CoC yang terdistribusi dan tahan manipulasi (*tamper-resistant*), di mana setiap perubahan atau akses terhadap bukti dicatat secara permanen dalam buku besar yang terenkripsi (Haji et al., 2026).

Namun, kemajuan teknologi CoC berhadapan langsung dengan dinding anonimitas pelaku yang semakin lihai. Penggunaan *cryptocurrency* sebagai alat transaksi ilegal dan teknik enkripsi *end-to-end* membuat identifikasi pelaku menjadi sangat sulit (Aini & Lubis, 2024). Dalam banyak kasus, penyidik berhadapan dengan data yang tersimpan di lingkungan awan (*cloud storage*) yang lokasinya tidak diketahui secara pasti atau berada di yurisdiksi asing (Karagiannis & Vergidis, 2021). Hal ini memicu pergeseran teori hukum dari penyitaan berbasis kepemilikan fisik menuju teori *"Power of Disposal"*. Teori ini berargumen bahwa penegak hukum harus memiliki otoritas untuk menguasai data berdasarkan kemampuan teknis untuk mengendalikan atau mengakses data tersebut, terlepas dari di mana server tersebut berada secara fisik (Karagiannis & Vergidis, 2021).

Perbandingan Metode	**Forensik Tradisional**	***Cloud Forensics & Power of Disposal***
Lokasi Data	Terlokalisasi pada perangkat fisik.	Tersebar secara dinamis *(data redundancy).*

Akses Bukti	Melalui penyitaan fisik perangkat.	Melalui otentikasi pengguna atau perintah penyedia layanan.
Tantangan Utama	Kerusakan fisik media penyimpanan.	Anonimitas pengguna dan enkripsi data.
Kedaulatan	Teritorialitas yang jelas.	Kehilangan lokasi fisik data *(loss of location).*

Sumber: Sintesis dari Karagiannis & Vergidis (2021).

Integrasi kecerdasan buatan (AI) dalam sistem peradilan juga menambah lapisan kompleksitas baru pada epistemologi bukti. AI dapat membantu dalam analisis skala besar terhadap data ilegal, namun transparansi algoritmanya sering kali dipertanyakan (Rodríguez-Salcedo et al., 2025). Risiko bias algoritma dan kurangnya penjelasan mengenai bagaimana sistem AI mencapai kesimpulan tertentu dapat merusak prinsip keadilan prosedural (Rodríguez-Salcedo et al., 2025). Oleh karena itu, *Digital Justice* menuntut adanya pengawasan manusia yang bermakna (*meaningful human oversight*) dalam penggunaan alat bantu otomatis untuk memastikan bahwa keputusan yudisial tidak didasarkan pada proses "kotak hitam" yang tidak dapat dipertanggungjawabkan (Rodríguez-Salcedo et al., 2025).

Kesimpulannya, pembuktian di era digital memerlukan lebih dari sekadar pembaruan teknis; ia memerlukan redefinisi hukum mengenai apa yang membentuk "kebenaran materiil." Sinkronisasi antara standar teknis internasional dengan regulasi nasional seperti UU ITE dan UU PDP di Indonesia menjadi prasyarat mutlak. Tanpa protokol standar yang diakui secara universal, penegakan hukum pidana siber akan terus terjebak dalam ketidakpastian antara kebutuhan untuk menindak kejahatan dan kewajiban untuk menjaga integritas proses peradilan (Rakha, 2024).

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Dialektika Kedaulatan Siber dan Jurisdiksi: Transformasi Penegakan Hukum dari Teritorialitas ke Virtualitas

Penegakan hukum pidana siber tidak hanya berhadapan dengan kebuntuan teknis pembuktian, tetapi juga tantangan ontologis terhadap konsep kedaulatan negara. Secara tradisional, kedaulatan negara berakar pada wilayah geografis yang tetap (teritorialitas), namun internet menciptakan ruang virtual yang melampaui batas-batas nasional (SHOKRI, 2025). Hal ini menciptakan apa yang disebut sebagai krisis yurisdiksi, di mana kejahatan dapat dimulai di satu negara, melewati server di sepuluh negara lain, dan menimbulkan dampak merugikan di negara tujuan yang jauh (SHOKRI, 2025).

Lawrence Lessing, dalam tesisnya yang terkenal *"Code is Law,"* mengemukakan bahwa di ruang siber, regulasi tidak hanya dilakukan melalui hukum formal, tetapi juga melalui arsitektur teknis yang membentuk lingkungan tersebut (Lessig, 2006). Lessing mengidentifikasi empat modalitas regulasi yang bekerja secara simultan untuk membentuk perilaku di dunia digital: hukum, norma sosial, pasar, dan arsitektur (kode) (Cohen, 2012). Di era anonimitas, kode menjadi regulator yang paling dominan; misalnya, penggunaan enkripsi yang kuat adalah bentuk "kode" yang menentang "hukum" negara untuk melakukan pengawasan (Lessig, 2000).

Modalitas Regulasi *(Lessing)*	**Mekanisme Kerja**	**Dampak pada Penegakan Hukum**
Hukum	Perintah negara yang disertai sanksi pidana.	Seringkali tertinggal oleh kecepatan inovasi teknologi.
Kode (Arsitektur)	Batasan teknis yang tertanam dalam perangkat lunak/keras.	Menentukan apakah anonimitas mungkin dilakukan atau tidak.
Norma	Tekanan sosial dan etika komunitas pengguna.	Mengatur perilaku yang tidak terjangkau oleh sensor formal.
Pasar	Harga, ketersediaan, dan insentif ekonomi.	Memengaruhi akses individu terhadap alat enkripsi/anonimitas.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Sumber: Diolah dari Lessig (2006).

Konflik kedaulatan ini semakin meruncing melalui persaingan dua teori besar dalam tata kelola siber global: Teori *Global Commons* dan Teori *Cyber Sovereignty*. Teori *Global Commons*, yang banyak dianut oleh negara-negara Barat, memandang ruang siber sebagai milik bersama umat manusia yang harus tetap terbuka dan bebas dari campur tangan negara yang berlebihan (Chuanying, 2016). Sebaliknya, Teori *Cyber Sovereignty*, yang dipromosikan oleh Tiongkok dan Rusia, menegaskan bahwa negara memiliki hak kedaulatan penuh untuk mengatur infrastruktur digital, data, dan konten di dalam batas wilayah mereka (SHOKRI, 2025).

Persaingan teori ini berdampak langsung pada bagaimana yurisdiksi kriminal diterapkan. Negara-negara mulai mengadopsi prinsip yurisdiksi extraterritorial untuk menjangkau pelaku kejahatan siber yang berada di luar negeri. Namun, pelaksanaan yurisdiksi penegakan (*enforcement jurisdiction*) tetap terbatas pada kedaulatan negara lain (SHOKRI, 2025). Hal ini menyebabkan beralihnya ketergantungan penegak hukum pada mekanisme kerja sama internasional seperti *Mutual Legal Assistance Treaties* (MLAT). Sayangnya, MLAT sering dianggap terlalu lambat untuk menangani bukti digital yang volatil (Shurson, 2025). Sebagai solusinya, instrumen seperti *US CLOUD Act* dan *EU e-Evidence Regulation* mulai diperkenalkan untuk memungkinkan akses langsung ke data yang dikuasai oleh penyedia layanan swasta lintas batas (Shurson, 2025).

Konsep *Digital Justice* yang diusung oleh Katsh dan Rabinovich-Einy menekankan bahwa teknologi harus digunakan sebagai alat untuk meningkatkan akses terhadap keadilan melalui *Online Dispute Resolution* (ODR). Namun, dalam konteks pidana, Richard Susskind memperingatkan bahwa transisi ke pengadilan daring (*Online Courts*) membawa tantangan filosofis (Dickson, 2020). Ada kekhawatiran bahwa persidangan virtual dapat mengurangi martabat proses peradilan dan mengabaikan hak-hak terdakwa yang mengalami "kerentanan digital" (*digital vulnerability*) (Dickson, 2020). Misalnya,

individu yang tidak memiliki akses internet stabil atau literasi teknologi yang memadai mungkin tidak dapat berpartisipasi secara efektif dalam pembelaan diri mereka (Sedláček et al., 2026).

Selain itu, prinsip peradilan yang jujur dan adil (*fair trial*) sebagaimana diatur dalam Pasal 6 ECHR menghadapi ujian berat dalam sistem peradilan digital. Transparansi proses peradilan, hak untuk memeriksa bukti secara langsung, dan hak atas keputusan yang beralasan dapat terganggu jika sistem peradilan mulai sangat bergantung pada algoritma yang tidak transparan (Sedláček et al., 2026). Richard Susskind berargumen bahwa tantangan kita bukan pada apakah teknologi harus digunakan, melainkan pada bagaimana memastikan bahwa penggunaan teknologi tersebut mewakili perbaikan atas sistem tradisional, bukan sekadar digitalisasi dari ketidakadilan yang sudah ada (Dickson, 2020).

Dalam konteks Indonesia, tantangan ini menuntut sinkronisasi yang lebih dalam antara UU ITE, UU PDP, dan KUHAP untuk menciptakan kerangka kerja yang harmonis bagi penegakan hukum siber (Firdaus, 2024). Perlindungan data pribadi tidak boleh dilihat sebagai penghambat investigasi, melainkan sebagai bagian integral dari keadilan digital yang melindungi hak asasi manusia dari penyalahgunaan kekuasaan oleh negara maupun aktor non-negara (Bigo et al., 2012). Upaya untuk mencapai keamanan siber nasional harus diseimbangkan dengan perlindungan terhadap privasi dan anonimitas yang sah, sebagaimana diakui dalam diskursus hak asasi manusia internasional (Rakha, 2024).

Secara keseluruhan, dialektika antara kedaulatan siber dan yurisdiksi virtual menunjukkan bahwa penegakan hukum di era digital memerlukan lebih dari sekadar kerja sama teknis; ia memerlukan kesepakatan normatif global mengenai batas-batas kekuasaan negara di ruang siber. *Digital Justice* hanya dapat tercapai jika hukum mampu menyesuaikan diri dengan arsitektur kode tanpa kehilangan komitmennya terhadap prinsip-prinsip dasar keadilan dan supremasi hukum. Transformasi dari "teritorialitas" ke

"virtualitas" adalah sebuah keniscayaan, dan keberhasilan kita dalam menavigasi transisi ini akan menentukan legitimasi sistem peradilan pidana di abad ke-21.

4. KESIMPULAN

Berdasarkan analisis mendalam yang telah dilakukan, penelitian ini menyimpulkan bahwa *Digital Justice* di era anonimitas siber merupakan sebuah tantangan multidimensional yang memerlukan reorientasi fundamental dalam hukum pidana dan hukum acara. Tantangan pembuktian digital bukan sekadar masalah teknis ekstraksi data, melainkan krisis epistemologis mengenai validitas dan integritas bukti dalam ekosistem yang volatil dan terenkripsi. Penggunaan protokol rantai penjagaan (*Chain of Custody*) yang didukung teknologi *blockchain* dan adopsi teori *"Power of Disposal"* muncul sebagai solusi potensial untuk menjembatani kesenjangan antara hukum teritorial konvensional dan realitas data virtual lintas batas.

Lebih lanjut, dialektika kedaulatan menunjukkan bahwa negara tidak lagi dapat mengandalkan yurisdiksi teritorial yang kaku. Tesis *"Code is Law"* dari Lawrence Lessing mempertegas bahwa penegakan hukum harus mampu berinteraksi dengan arsitektur siber itu sendiri melalui kolaborasi dengan sektor swasta dan sinkronisasi regulasi internasional. Namun, transformasi menuju peradilan digital harus tetap dipandu oleh prinsip keadilan prosedural untuk mencegah eksklusi digital dan bias algoritma yang dapat merugikan hak-hak dasar terdakwa. Indonesia, melalui UU ITE dan UU PDP, harus terus memperkuat integritas sistem hukum sibernya agar mampu menghadapi ancaman anonimitas pelaku tanpa mengorbankan perlindungan data pribadi dan hak asasi manusia. Keberhasilan pencapaian keadilan digital pada akhirnya bergantung pada kemampuan kita untuk mengintegrasikan inovasi teknologi dengan nilai-nilai luhur kemanusiaan dalam setiap proses penegakan hukum pidana.

5. REFERENSI

A., M. Y. (2010). Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime. *Pranata Hukum*, *5*(2), 77–90. https://media.neliti.com/media/publications/26724-ID-pembuktian-dalam-hukum-pidana-indonesia-terhadap-cyber-crime.pdf

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(2), 55–63. https://doi.org/10.54209/judge.v5i02.566

Badiye, A., Kapoor, N., & Menezes, R. G. (2023). *Chain of Custody*. StatPearls Publishing.

Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J., & Scherrer, A. (2012). *Fighting cyber crime and protecting privacy in the cloud*. European Union.

Chuanying, L. (2016). *Cyber strategies of great powers: US-China interactions and cooperation*. SIIS. https://www.siis.org.cn/Commentary/2211.jhtml

Cohen, J. E. (2012). "Piracy," "Security," and Architectures of Control. *Configuring the Networked Self*, *7*, 1–28.

Dickson, D. A. (2020). *Review of Online Courts and the Future of Justice (Susskind)*. Oxford University Press. https://www.lawscot.org.uk/members/journal/issues/vol-65-issue-01/book-reviews/

Farhan, Hamdani, F., Astuti, N. L. V. P., Fiqry, H. A. H., & Aulia, M. R. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Jurnal Indonesia Berdaya*, *3*(3), 567–576.

Firdaus, R. A. (2024). Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia. *Staatsrecht: Jurnal Kenegaraan Dan Politik Islam*, *4*(1). https://doi.org/10.14421/cf582q68

Haji, I. A., Mohammed, S. D., & Mousa, K. M. (2026). Blockchain based chain of custody and digital evidence legality in post conflict prosecutions. *Frontiers Media SA*, *9*. https://doi.org/10.3389/fbloc.2026.1801364

Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information*, *12*(5). https://doi.org/10.3390/info12050181

Lessig, L. (2000). *Lawrence Lessig on the increasing regulation of cyberspace*. https://www.harvardmagazine.com/2000/01/code-is-law-html

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books.

Marzuki, P. M. (2014). *Metode Penelitian Hukum*. Kencana Prenada Media Group.

Novita, D., Mulyono, & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *INNOVATIVE: Journal Of Social Science Research*, *4*(6), 1179–1186.

Prasad, A. (2025). The Rise of Cyber Crime – How Digital Evidence is Changing Investigation. *The Lawway with Lawyers Journal*, *29*(29). https://thelawwaywithlawyers.com/the-rise-of-cyber-crime-how-digital-evidence-is-changing-investigation/

Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, *16*(2). https://doi.org/10.22201/iij.24485306e.2024.2.18892

Rodríguez-Salcedo, E., Bonilla, C. A. M., Mayorga, B. P., Salame, M., Freire, P. V. A., Miniguano, A. E., & Pino, E. (2025). Evaluating AI decision tools in Ecuador's courts: efficiency, consistency, and uncertainty in legal judgments. *Technology and Law*, *8*. https://doi.org/10.3389/frai.2025.1688209

Sedláček, M., Střeleček, T., Kotápišová, P., Mareková, M., Navrátil, P., & Hořeňovský, J. (2026). Digital Resolution of Civil Disputes: Procedural Guarantees and Judicial Decision-Making. *The Lawyer Quarterly*, *16*(1), 48–66. https://tlq.ilaw.cas.cz/index.php/tlq/article/view/684

SHOKRI, A. (2025). Sovereignty in Cyberspace from the Viewpoint of International Law. *Asian Journal of International Law*, 1–31. https://doi.org/10.1017/S2044251325100556

Shurson, J. (2025). Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations. *International and Comparative Law Quarterly*, *74*(3), 675–705. https://doi.org/10.1017/S0020589325100985

Silalahi, J. A. S. (2023). The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities. *INNOVATIVE: Journal Of Social Science Research*, *3*(2), 3658–3668. https://j-innovative.org/index.php/Innovative/article/view/678

Sufian, J., & Eddyono, S. W. (2024). *Penyelidikan dan Penyidikan Terhadap Anonimitas Pelaku Kejahatan Siber di Indonesia* [Universitas Gadjah Mada]. https://etd.repository.ugm.ac.id/penelitian/detail/243609

Taher, B., Towfiq, T. A., & Mousa, K. (2025). Cybercrime: A Phenomenon Challenging

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Criminal Justice: A Legal Analytical Study. *American Journal of Society and Law*, *4*(2), 11–14. https://doi.org/10.54536/ajsl.v4i2.6145