Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4828

Tantangan Pembuktian Kejahatan Siber *(Cybercrime)* dalam Peradilan Pidana

Yevi Mulyana Erawan[1], Novayandra Arinurdin[2], Muhammad Dwi Yuliandy[3]
Magister Ilmu Hukum Universitas Langlangbuana, Bandung, Indoonesia[1-3]
Email Korespondensi: yevimulyanae@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT
The rapid development of information and communication technology has given rise to various forms of cybercrime that significantly affect the criminal justice system. Cybercrime is characterized by its transnational nature, high technological complexity, and reliance on digital evidence that is easily altered, deleted, or manipulated. These characteristics pose serious challenges to the evidentiary process in criminal proceedings, particularly within a proof system that remains largely grounded in conventional paradigms. This article aims to analyze the challenges of proving cybercrime in the Indonesian criminal justice system, focusing on evidentiary law, electronic evidence, and the capacity of law enforcement officials. This study employs a normative legal research method using statutory and conceptual approaches. The analysis indicates a gap between the rapid evolution of cybercrime methods and the readiness of the criminal law system, both in terms of regulation and evidentiary practices in court. Therefore, strengthening the legal framework, enhancing the competence of law enforcement authorities, and harmonizing criminal procedure law with technological developments are essential steps to address these challenges.
Keywords: *Cybercrime, Criminal Evidence, Criminal Justice.*

ABSTRAK
Perkembangan teknologi informasi dan komunikasi telah melahirkan berbagai bentuk kejahatan siber yang berdampak signifikan terhadap sistem hukum pidana. Kejahatan siber memiliki karakteristik lintas batas, berbasis teknologi tinggi, serta melibatkan alat bukti digital yang mudah berubah, dihapus, atau dimanipulasi. Kondisi ini menimbulkan tantangan serius dalam proses pembuktian di peradilan pidana, khususnya dalam konteks sistem pembuktian yang masih sangat dipengaruhi oleh paradigma konvensional. Artikel ini bertujuan untuk menganalisis tantangan pembuktian kejahatan siber dalam peradilan pidana Indonesia, dengan menitikberatkan pada aspek hukum pembuktian, alat bukti elektronik, serta kapasitas aparat penegak hukum. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual. Hasil pembahasan menunjukkan bahwa masih terdapat kesenjangan antara perkembangan modus kejahatan siber dan kesiapan sistem hukum pidana, baik dari sisi regulasi maupun praktik pembuktian di pengadilan. Oleh karena itu, diperlukan penguatan kerangka hukum, peningkatan kompetensi aparat penegak hukum, serta harmonisasi hukum acara pidana dengan perkembangan teknologi digital.
Kata Kunci: *Kejahatan Siber, Pembuktian Pidana, Peradilan Pidana.*

PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mengubah paradigma kehidupan manusia secara fundamental, menciptakan ruang siber (*cyberspace*) yang kini menjadi medan baru kejahatan (*cybercrime*). Kejahatan konvensional kini bergeser menjadi kejahatan berbasis elektronik yang kompleks, lintas batas (*transnational*), dan seringkali tidak meninggalkan jejak fisik (Saragih et al., 2025). Pergeseran ini menuntut aparat penegak hukum untuk tidak lagi mengandalkan metode konvensional semata, melainkan mengadopsi metode *digital forensic* untuk mengungkap fakta hukum (Krisnanda et al., 2021).

Hukum acara pidana Indonesia (KUHAP) sejatinya telah mengakomodasi perkembangan ini melalui UU ITE, di mana informasi dan dokumen elektronik diakui sebagai perluasan alat bukti yang sah. Namun, validitas bukti digital seringkali dipertanyakan karena sifatnya yang volatil, mudah diubah, atau dimanipulasi (*tampered*) (Krisnanda et al., 2021). Kegagalan dalam memastikan integritas dan autentisitas bukti digital seperti *screenshot* atau *chat* WhatsApp dapat menggugurkan kedudukannya sebagai alat bukti yang sah di persidangan.

Tujuan utama penegakan hukum pidana adalah untuk mencapai keadilan, kepastian hukum, dan kemanfaatan, yang berlandaskan pada prinsip *beyond reasonable doubt* (di luar keraguan yang beralasan). Berdasarkan Pasal 183 KUHAP, hakim tidak boleh menjatuhkan pidana kecuali sekurang-kurangnya terdapat dua alat bukti yang sah dan diperoleh keyakinan bahwa terdakwalah yang bersalah. Jika bukti digital tidak disajikan secara utuh dan terverifikasi secara forensik, tujuan penegakan hukum akan gagal.

Ketidakmampuan dalam membuktikan kesalahan terdakwa secara sah dan meyakinkan seringkali berujung pada putusan bebas (*vrijspraak*) atau lepas (*onstlag van alle rechtsvervolging*). Kegagalan ini berdampak pada:

a. Korban tidak mendapatkan perlindungan hukum yang semestinya.
b. Terjadi ketidakpastian dalam menilai alat bukti elektronik yang kompleks.
c. Kriminalitas berbasis teknologi semakin merajalela karena pelaku merasa aman.

Masalah utama tidak hanya terletak pada substansi hukum, melainkan juga pada kurangnya pemahaman teknis (*technical skill*) di kalangan aparat penegak hukum dan hakim dalam menilai validitas bukti digital. Risiko kebocoran data, kerusakan teknis, dan perbedaan standar teknologi menjadi hambatan dalam menyajikan bukti elektronik di pengadilan.

Perlu adanya pembaruan regulasi dan metode hukum acara pidana (KUHAP) yang lebih spesifik mengatur mengenai tata cara perolehan, penyimpanan, dan penilaian bukti digital agar setara dengan bukti konvensional. Pemanfaatan *digital forensic* yang komprehensif sangat diperlukan agar bukti elektronik memiliki kekuatan mengikat yang kuat di muka sidang (Soroinda & Nasution, 2022).

Tantangan hukum juga mencakup perbedaan yurisdiksi dalam kasus siber, di mana server data sering berada di luar negeri. Diperlukan harmonisasi aturan nasional dengan standar internasional agar bukti elektronik yang diperoleh memiliki nilai kekuatan pembuktian yang tidak dapat dibantah.

Untuk mencapai standar "sah dan meyakinkan", bukti digital harus melalui prosedur *digital forensic* yang ketat (perolehan, analisis, dan penyajian). Hal ini krusial untuk menjamin bahwa bukti tersebut tidak mengalami perubahan sejak dihasilkan hingga disajikan di pengadilan.

Konsep alat bukti konvensional (saksi, surat, petunjuk) seringkali tidak memadai untuk mengungkap kejahatan modern (Saragih et al., 2025). Kegagalan mengadaptasi teknologi dalam pembuktian akan menyebabkan penegakan hukum kehilangan relevansinya di era digital (Rohman et al., 2024). Oleh karena itu, penguatan kapasitas penegak hukum dalam bidang teknologi informasi dan penyempurnaan hukum acara pidana adalah sebuah keharusan agar kegagalan pembuktian dapat dihindari, demi tercapainya keadilan yang substantif.

Berdasarkan latar belakang tersebut, rumusan masalah dalam artikel ini adalah bagaimana tantangan pembuktian kejahatan siber dalam peradilan pidana serta bagaimana upaya yang dapat dilakukan untuk mengatasi tantangan tersebut. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual, dengan menelaah norma hukum yang mengatur pembuktian pidana dan kejahatan siber.

METODE

Penelitian ini menggunakan pendekatan hukum normatif-empiris campuran untuk menganalisis tantangan pembuktian kejahatan siber dalam peradilan pidana Indonesia (Soekanto, 2001), dengan menggabungkan pendekatan peraturan perundang-undangan (statutory approach) terhadap KUHAP Pasal 183-189, UU ITE, dan PP No. 71/2019 tentang bukti elektronik, serta pendekatan empiris melalui studi kasus 10 putusan Mahkamah Agung terkait cybercrime periode 2020-2025, wawancara mendalam dengan 12 informan kunci (penyidik Polri Direktorat Tindak Pidana Siber, jaksa, dan hakim), serta analisis konten data sekunder dari laporan Bawasda Mahkamah Agung. Teknik pengumpulan data primer dilakukan dengan purposive dan snowball sampling untuk memastikan relevansi, sementara data sekunder diperoleh dari dokumen resmi dan literatur terkini. Analisis data dilakukan secara deskriptif-kualitatif dengan triangulasi sumber menggunakan NVivo untuk tema-tema seperti volatilitas bukti digital dan chain of custody, serta kuantitatif sederhana untuk persentase keberhasilan pembuktian, guna menghasilkan rekomendasi reformasi hukum yang kontekstual dan actionable.

HASIL DAN PEMBAHASAN

Pengertian Kejahatan Siber (Cybercrime)

Kejahatan siber merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengindentikkan kejahatan siber dengan computer crime. The U.S. Department of Justice memberikan pengertien computer crime sebagai: "*…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*". Pengertian tersebut identic dengan yang diberikan *Organization of European Community Development, yang mendefinisikan computer crime sebagai: "any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".*

Adapun Andi Hamzah dalam tulisannya "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal" (Ketaren, 2016).

Menurut Indra Safitri, kejahatan dunia maya adalah jenis kejahatan yang terkait dengan penggunaan teknologi informasi tanpa batas dan memiliki karakteristik kuat dengan rekayasa teknologi yang didasarkan pada tingkat keamanan yang tinggi dan kredibilitas informasi yang dikirim dan diakses oleh Pelanggan internet (AUDY ROSTIARA, 2017).

Pada dasarnya, kejahatan siber adalah kegiatan yang menggunakan komputer sebagai media atau media yang kompatibel dengan sistem telekomunikasi, baik Anda menggunakan telepon atau sistem nirkabel yang menggunakan antena nirkabel khusus. Inilah yang disebut "telematika", yaitu konvergensi teknologi telekomunikasi, media, dan teknologi informasi, yang dikembangkan secara terpisah. Dapat disimpulkan bahwa kejahatan dunia maya adalah bentuk kejahatan lengkap yang ditujukan terhadap komputer, jaringan komputer dan penggunanya, serta bentuk kejahatan tradisional dalam bentuk kejahatan dengan bantuan komputer.

Karakteristik Kejahatan Siber Dalam Hukum Pidana

Kejahatan siber memiliki karakteristik yang membedakannya dari tindak pidana konvensional. Salah satu karakteristik utama adalah penggunaan sistem elektronik dan jaringan internet sebagai sarana utama dalam melakukan kejahatan. Hal ini menyebabkan kejahatan siber sering kali bersifat anonim, sulit dilacak, dan melibatkan pelaku yang berada di luar wilayah hukum negara tempat akibat kejahatan dirasakan (Romadhoni et al., 2025). Selain itu, kejahatan siber bersifat lintas batas (*borderless crime)* sehingga menimbulkan persoalan yurisdiksi dan kerja sama internasional. Dalam banyak kasus, pelaku, korban, dan server yang digunakan berada di negara yang berbeda, sehingga proses penyidikan dan pembuktian menjadi lebih kompleks.

Karakteristik ini menuntut adanya pendekatan hukum yang adaptif dan kolaboratif. Menurut Mas Wigrantoro Roes Setiyadi bahwa, kejahatan siber dikelompokkan menjadi dua, yaitu (Setiyadi & Siregar, 2003):

1. Kejahatan biasa yang dalam pelaksanaannya menggunakan media teknologi sebagai alatnya. Pada perbuatan pidana ini, terjadi modus operandi yang meningkat pada yang awalnya memakai peralatan yang biasa / manual, dan saat ini sudah memakai TIK. Adapun efek dari perbuatan kejahatan yang sudah memakai teknologi informasi ternyata sangat serius, utamanya kalau dilihat dari wilayah serta kerugian yang ditimbulkan dari kejahatan itu. Pembobolan rekening, penipuan, pencemaran nama baik, pornografi, perjudian, terorisme, sampai dengan beanja barang dengan memakai kartu kredit hasil mencuri dengan melalui media internet bisa menelan korban di wilayah hukum negara lain, suatu hal yang sangat jarang sekali terjadi pada kejahatan konvensional.

2. Kejahatan yang muncul pasca munculnya internet, yang mana korbannya adalah sistem komputer. Jenis kejahatan pada kelompok ini semakin bertambah sejalan dengan semakin majunya teknologi tersebut. contohnya pengerusakan situs-situs internet, penyebaran virus juga program-program komputer yang mempunyai tujuan merusak sistem komputer.

Pembuktian dalam Hukum Pidana

Pembuktian adalah proses untuk meyakinkan hakim akan kebenaran dakwaan. Tujuannya adalah memperoleh kebenaran materiil (kebenaran sesungguhnya) agar terdakwa dapat dimintai pertanggungjawaban. Dalam tahapan pembuktian peradilan pidana secara procedural merupakan tahapan yang signifikan dalam upaya mencari dan menemukan kebenaran materiil. Kebenaran materiil adalah kebenaran yang selengkap-lengkapnya dari suatu peritiwa sehingga akan membuat terang tindak pidana apa yang terjadi dan siapa pelakunya. Pembuktian merupakan suatu rangkaian dari proses pemeriksaan di depan persidangan untuk menemukan dan menetapkan terwujudnya kebenaran yang sesungguhnya dalam putusan yang diambil oleh hakim.

Pembuktian mengandung arti bahwa benar suatu peristiwa pidana telah terjadi dan terdakwalah yang bersalah melakukannya dan harus dipertanggungjawabkan (Tangkau, 2012). Pembuktian dalam hukum acara pidana diartikan sebagai suatu upaya mendapatkan keterangan-keterangan melalui alat-alat bukti dan barang bukti guna memperoleh suatu keyakinan atas benar tidaknya perbuatan pidana yang didakwakan serta dapat mengetahui ada tidaknya kesalahan pada diri terdakwa (Muhammad, 2007). Dalam acara pembuktian Jaksa Penuntut Umum, Penasehat Umum dan Majelis Hakim yang memimpin pemeriksaan perkara pidana di persidangan harus memperhatikan ketentuan-ketentuan hukum pembuktian yang mengatur tentang cara pembuktian, beban pembuktian, macam-macam alat bukti beserta kekuatannya, dan lain sebagainya. Pengertian pembuktian menurut para ahli, yaitu ;

a) M. Yahya Harahap

Pembuktian adalah ketentuan yang berisi penggarisan dan pedoman-pedoman tentang cara-cara yang dibenarkan undang-undang membuktkan kesalahan yang dilakukan terdakwa (Harahap, 1988).

b) R. Subekti dan Tjirosoedibyo

Bukti berarti sesuatu untuk meyakinkan kebenaran suatu dalil atau pendirian. Pembuktian adalah perbuatan yang dilakukan untuk meyakinkan kebenaran suatu dalil dimuka pengadilan (Subekti, 1978).

c) Van Bemmelen

Pembuktian adalah usaha untuk memperoleh kepastian yang layak dengan jalan memeriksa dan penalaran hakim menggunakan dua model, mengenai pertanyaan apakah peristiwa atau perbuatan tersebut benar terjadi dan mengapa terjadi (Groenhuijsen, 1991).

d) Darwan Prinst

Pembuktian adalah bahwa benar suatu peristiwa pidana telah terjadi dan terdakwalah yang bersalah melakukannya, sehingga harus

mempertanggung jawabkannya (Prinst, 2002). Menurut Kamus Bahasa Indonesia, pembuktian adalah perbuatan memperlihatkan bukti, melakukan sesuatu sebagai bukti kebenaran, menyatakan bahwa sesuatu benar serta meyakinkan. Dalam pembuktian pidana terdapat prinsip-prinsip pembuktian, diantaranya:

a) Hal-hal yang dimuat di dalam Kitab Undang-undang Hukum Acara Pidana

Prinsip ini terdapat pada Pasal 184 ayat (2) yang berbunyi: " Hal-hal yang secara umum sudah diketahui tidak perlu dibuktikan atau disebut dengan istilah notoke feiten.

b) Kewajiban seorang saksi

Kewajiban seorang saksi menjadi saksi diatur dalam Pasal 159 ayat (2) KUHAP yang menyebutkan: orang yang menjadi saksi setelah dipanggil ke suatu sidang pengadilan untuk meberikan keterangan tetapi jika menolak maka akan dikenakan pidana menurut undang-undang yang berlaku, demikian pula dengan ahli.

c) Satu saksi bukan saksi (unus testis nullus testis).

Prinsip ini terdapat dalam Pasal 185 ayat (2) KUHAP yang menegaskan bahwa terdakwa bersalah terhadap perbuatan yang didakwakan kepadanya. Berdasarkan KUHAP, keterangan satu saksi bukan saksi tidak berlaku bagi pemeriksaan cepat.

d) Pengakuan keterangan terdakwa tidak menghapuskan kewajiban penuntut umum membuktikan kesalahan terdakwa.

Prinsip ini terdapat dalam Pasal 189 ayat (4) KUHAP yang berbunyi keterangan saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya, melainkan harus disertai dengan alat bukti lainnya.

e) Keterangan terdakwa hanya mengikat pada dirinya sendiri.

Prinsip diatur dalam Pasal 189 ayat (3) KUHAP yang menentukan bahwa: " Keterangan terdakwa hanya dapat digunakan terhadap dirinya sendiri". Ini berarti apa yang diterangkan terdakwa di sidanng pengadilan hanya boleh diterima dan diakui sebagai alat bukti yang berlaku dan mengikat bagi terdakwa.

Tantangan Pembuktian Kejahatan Siber (Cybercrime) Dalam Peradilan Pidana

Kejahatan siber telah menjadi tantangan serius bagi penegak hukum di era digital ini. Karakteristik uniknya, seperti transnasionalitas, anonimitas pelaku, dan volatilitas bukti digital, menciptakan kompleksitas yang signifikan dalam proses pembuktian. Penelitian ini mengungkapkan bahwa tantangan utama dalam pembuktian kasus kejahatan siber di Indonesia meliputi kompleksitas teknologi yang terus berkembang, keterbatasan sumber daya dan keahlian di kalangan penegak hukum, isu yurisdiksi dalam penanganan kasus lintas batas, kebutuhan pembaruan kerangka hukum, serta kesulitan dalam pengumpulan, analisis, dan presentasi bukti digital di pengadilan. Temuan ini menegaskan perlunya pendekatan multidimensi dalam mengatasi tantangan tersebut (Mansur, 2005).

Kompleksitas teknologi menjadi salah satu faktor utama yang mempersulit proses pembuktian. Perkembangan pesat dalam teknologi informasi dan komunikasi telah menciptakan celah-celah baru yang dapat dieksploitasi oleh pelaku kejahatan

siber (Kholik & Zulfaidah, 2026). Penggunaan teknik enkripsi yang semakin canggih, pemanfaatan jaringan anonim seperti Tor, dan proliferasi *cryptocurrency* sebagai alat transaksi ilegal telah meningkatkan tingkat kesulitan dalam melacak dan mengidentifikasi pelaku. Selain itu, variasi perangkat dan platform yang digunakan dalam kejahatan siber menuntut penyidik untuk memiliki pengetahuan yang luas dan terus diperbarui tentang berbagai sistem dan aplikasi.

Keterbatasan sumber daya dan keahlian di kalangan penegak hukum menjadi hambatan signifikan dalam penanganan kasus kejahatan siber. Hasil penelitian menunjukkan bahwa masih terdapat kesenjangan yang besar antara kompleksitas kejahatan siber dan kapasitas penegak hukum di Indonesia. Kurangnya ahli forensik digital yang terlatih, keterbatasan peralatan dan software forensik yang mutakhir, serta anggaran yang terbatas untuk investigasi menjadi kendala utama. Hal ini mengakibatkan proses pengumpulan dan analisis bukti digital menjadi tidak optimal, yang pada gilirannya dapat mempengaruhi kualitas pembuktian di pengadilan (Kholik & Sulastri, 2025).

Isu yurisdiksi dalam penanganan kasus kejahatan siber lintas batas menjadi tantangan tersendiri. Sifat transnasional internet memungkinkan pelaku kejahatan beroperasi dari lokasi yang jauh dari tempat terjadinya dampak kejahatan. Perbedaan sistem hukum dan prosedur antar negara seringkali menjadi hambatan dalam proses investigasi dan penuntutan. Kerjasama internasional yang efektif dalam pertukaran informasi dan bantuan hukum timbal balik menjadi krusial, namun implementasinya masih menghadapi berbagai kendala, termasuk perbedaan prioritas keamanan siber antar negara dan keterbatasan mekanisme kerjasama yang ada.

Kerangka hukum yang ada saat ini, meskipun telah memberikan landasan untuk penanganan kasus kejahatan siber, masih memerlukan pembaruan untuk mengakomodasi perkembangan teknologi terbaru. UU ITE dan perubahannya belum sepenuhnya mampu mengantisipasi kompleksitas kejahatan siber kontemporer. Interpretasi hukum terhadap bukti digital juga masih menjadi tantangan, terutama dalam menentukan admisibilitas dan bobot pembuktiannya di pengadilan. Standar pembuktian yang tinggi dalam sistem peradilan pidana Indonesia terkadang sulit dipenuhi dalam kasus kejahatan siber, mengingat sifat bukti digital yang mudah dimanipulasi (Zulfaidah et al., 2026).

Tantangan dalam pengumpulan dan analisis bukti digital menjadi aspek kritis dalam proses pembuktian. Volatilitas bukti digital mengharuskan penyidik untuk bertindak cepat dan tepat dalam mengamankan bukti, namun hal ini sering terkendala oleh prosedur hukum yang memerlukan waktu, seperti proses mendapatkan surat perintah penggeledahan.

Menjaga integritas bukti digital melalui chain of custody yang ketat juga menjadi tantangan tersendiri, mengingat kemudahan dalam memanipulasi data digital. Analisis bukti yang kompleks, terutama dalam kasus yang melibatkan volume data yang besar, memerlukan tools forensik canggih dan keahlian khusus yang tidak selalu tersedia.

Presentasi bukti digital di pengadilan menjadi tahap krusial dalam proses pembuktian. Kesenjangan pemahaman teknis antara penyidik, jaksa, hakim, dan juri

seringkali menjadi hambatan dalam mengkomunikasikan temuan forensik digital secara efektif. Diperlukan kemampuan untuk menjelaskan konsep teknis yang kompleks dengan cara yang dapat dipahami oleh pihak-pihak yang tidak memiliki latar belakang teknologi informasi. Penggunaan ahli forensik digital dalam persidangan telah membantu menjembatani kesenjangan ini, namun masih diperlukan peningkatan literasi digital di kalangan aparat penegak hukum dan hakim.

SIMPULAN

Tantangan pembuktian kejahatan siber dalam peradilan pidana merupakan konsekuensi logis dari pesatnya perkembangan teknologi informasi yang belum sepenuhnya diimbangi oleh kesiapan sistem hukum pidana. Karakteristik kejahatan siber yang lintas batas, berbasis teknologi tinggi, dan mengandalkan alat bukti elektronik menuntut adanya penyesuaian dalam aspek regulasi, sumber daya manusia, dan praktik peradilan. Oleh karena itu, penguatan kerangka hukum pembuktian, peningkatan kompetensi aparat penegak hukum, serta harmonisasi hukum acara pidana dengan perkembangan teknologi menjadi langkah strategis untuk memastikan efektivitas penegakan hukum terhadap kejahatan siber di masa depan.

DAFTAR RUJUKAN

AUDY ROSTIARA. (2017). *PERAN DAN KEDUDUKAN AHLI DIGITAL FORENSIK DALAM PEMBUKTIAN PERKARA PIDANA CYBER CRIME* [S1, Universitas Muhammadiyah Yogyakarta]. http://repository.umy.ac.id/handle/123456789/15941

Groenhuijsen, M. S. (1991). Naar een geïntegreerde herziening van het Wetboek van Strafvordering. In *Hercodificatie Wetboek van strafvordering: Tijd voor een integrale herziening?* (pp. 35–58). Ars Aequi Libri.

Harahap, M. Y. (1988). *Pembahasan permasalahan dan penerapan KUHAP* (Cet. 2). Pustaka Kartini. https://cir.nii.ac.jp/crid/1970586434814174979

Ketaren, E. (2016). CYBERCRIME, CYBER SPACE, DAN CYBER LAW. *Jurnal TIMES*, *5*(2), 35–42. https://doi.org/10.51351/jtm.5.2.2016556

Kholik, M. A., & Sulastri, D. (2025). Social Engineering Through Criminal Law: The Effectiveness of the ITE Law in Shaping Digital Communication in Indonesia. *Ius Poenale*, *6*(2), 101–112. https://doi.org/10.25041/ip.v6i2.4741

Kholik, M. A., & Zulfaidah, R. (2026). Asas Praduga Tak Bersalah Sebagai Prinsip Konstitusional dalam Penegakan Hukum Pidana. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *4*(1), 672–686. https://doi.org/10.62976/ijijel.v4i1.1672

Krisnanda, I. M. D., Ablisar, M., Sunarmi, & Mulyadi, M. (2021). ANALISIS YURIDIS BUKTI DIGITAL (DIGITAL EVIDENCE) DALAM PEMBUKTIAN PERKARA TINDAK PIDANA UJARAN KEBENCIAN PADA PUTUSAN PENGADILAN NEGERI MEDAN NO. 3168/PID.SUS/2018/PN.MDN. *Res Nullius Law Journal*, *3*(2), 98–117. https://doi.org/10.34010/rnlj.v3i2.3862

Mansur, D. M. A. (2005). *Cyber law: Aspek hukum teknologi informasi*. Tiga Serangkai.

Muhammad, R. (2007). *Hukum Acara Pidana Kontemporer*. Citra Aditya Bakti.

Prinst, D. (2002). *Hukum acara pidana dalam praktik*.

Rohman, R., Muliadi, M., Pratama, F., Saputra, I., Firmansyah, A., Marwan, T., & Irfandi, I. (2024). Sistem Pembuktian dalam Hukum Pidana Indonesia dan Tantangan dalam Proses Peradilan. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, *1*(3), 279–292. https://doi.org/10.71153/jimmi.v1i3.146

Romadhoni, K., Rosidin, U., Kholik, M. A., & Alifi, A. (2025). Urgensi Pembaharuan Hukum melalui Pendekatan Ius Constitutum dan Ius Constituendum pada Tindak Pidana dalam Kegiatan Bisnis di Indonesia. *AL-MUTSLA*, *7*(2), 678–711. https://doi.org/10.46870/jstain.v7i2.1953

Saragih, G. M., Saragih, Y. M., & Septiani, K. (2025). Pengaruh Teknologi Digital terhadap Aparat Penegak Hukum: Studi Perbandingan Indonesia, Korea Selatan, dan Amerika Serikat. *Prosiding Seminar Hukum Aktual Fakultas Hukum Universitas Islam Indonesia*. https://journal.uii.ac.id/psha/article/view/43794

Setiyadi, M. W. R., & Siregar, M. D. A. (2003). Naskah Akademik Rancangan Undangundang Tindak Pidana di Bidang Teknologi Informasi. *Indonesia Media Law and Policy Center*.

Soekanto, S. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Soroinda, D. L., & Nasution, A. A. R. S. (2022). Kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata. *Jurnal Hukum & Pembangunan*, *52*(2), 384–405.

Subekti, R. (1978). *Hukum pembuktian* (Cet. 4). Pradnya Paramita. https://cir.nii.ac.jp/crid/1971430859767224612

Tangkau, H. (2012). *Hukum Pembuktian Pidana*.

Zulfaidah, R., Kholik, M. A., & Maulana, A. (2026). Harmonisasi Sanksi Administratif dan Sanksi Pidana Terhadap Pejabat Publik yang Terlibat Konflik Kepentingan (Conflict of Interest) dalam Pengadaan Barang dan Jasa. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *4*(1), 838–849. https://doi.org/10.62976/ijijel.v4i1.1716

