Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

ANALISIS PERBANDINGAN PENGATURAN HUKUM PIDANA TERHADAP TINDAK KEJAHATAN SIBER DI INDONESIA DAN AMERIKA SERIKAT

Riyos Randa Situru[1]
Fakultas Hukum, Universitas Tarumanagara[1]
Email: riyos.207252013@stu.untar.ac.id[1]

Abstrak
Perkembangan teknologi informasi telah mendorong munculnya berbagai bentuk kejahatan siber yang semakin kompleks, transnasional, dan sulit ditangani melalui pendekatan hukum pidana konvensional. Penelitian ini bertujuan menganalisis persamaan dan perbedaan pengaturan hukum pidana terhadap kejahatan siber di Indonesia dan Amerika Serikat serta mengkaji peran institusi penegak hukum dalam menghadapi perkembangan cybercrime. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan komparatif. Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, doktrin hukum, literatur ilmiah, serta berbagai kebijakan yang berkaitan dengan penanggulangan kejahatan siber di kedua negara. Hasil penelitian menunjukkan bahwa Indonesia dan Amerika Serikat sama-sama mengakui alat bukti elektronik dan menerapkan yurisdiksi terhadap kejahatan siber lintas negara, namun memiliki perbedaan dalam struktur regulasi, kapasitas kelembagaan, dan model penegakan hukum. Amerika Serikat didukung sistem yang lebih terintegrasi dan sumber daya yang lebih maju, sedangkan Indonesia masih menghadapi tantangan pada aspek harmonisasi regulasi, kapasitas forensik digital, dan koordinasi kelembagaan. Oleh karena itu, diperlukan penguatan regulasi yang adaptif, peningkatan kompetensi aparat penegak hukum, serta kerja sama internasional yang lebih efektif guna menjawab dinamika kejahatan siber yang terus berkembang.
Kata Kunci: kejahatan siber, hukum pidana, perbandingan hukum.

Abstract
The rapid development of information technology has contributed to the emergence of increasingly complex, transnational, and sophisticated forms of cybercrime that challenge the effectiveness of conventional criminal law approaches. This study aims to analyze the similarities and differences in criminal law regulations governing cybercrime in Indonesia and the United States, as well as to examine the role of law enforcement institutions in addressing the evolving nature of cyber threats. The research employs a normative legal research method using statutory and comparative approaches. Data were collected through a literature review of legislation, legal doctrines, academic publications, and policy frameworks related to cybercrime regulation and enforcement in both countries. The findings indicate that Indonesia and the United States both recognize electronic evidence as a valid means of proof and apply jurisdictional principles

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

to transnational cyber offenses. However, significant differences exist in their regulatory structures, institutional capacities, and enforcement mechanisms. The United States benefits from a more integrated legal and institutional framework supported by advanced technological resources, whereas Indonesia continues to face challenges related to regulatory harmonization, digital forensic capabilities, and inter-agency coordination. Therefore, adaptive legal reforms, enhanced law enforcement competencies, and stronger international cooperation are essential to effectively respond to the rapidly evolving landscape of cybercrime.
Keywords*: cybercrime, criminal law, comparative law.*

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah merevolusi tatanan kehidupan masyarakat secara mendalam, sekaligus membuka celah bagi munculnya bentuk-bentuk kejahatan baru yang semakin canggih. Transformasi digital tidak hanya mempercepat transaksi ekonomi, komunikasi, dan pelayanan publik, tetapi juga menciptakan ruang siber yang rentan terhadap eksploitasi. Di era di mana aktivitas sehari-hari semakin bergantung pada platform digital, kejahatan siber (cybercrime) muncul sebagai ancaman serius yang melampaui batas konvensional. Pelaku kejahatan kini dapat beroperasi secara anonim, melintasi yurisdiksi negara, dan menimbulkan kerugian ekonomi, sosial, serta keamanan nasional dalam skala yang masif.[1]

Dalam upaya regulasi telah dilakukan, perkembangan hukum pidana dalam merespons fenomena kejahatan siber sering kali tidak sejalan dengan kecepatan inovasi teknologi yang terus berkembang. Berbagai ketentuan hukum yang dibentuk cenderung hadir setelah suatu permasalahan muncul, sehingga lebih bersifat responsif daripada antisipatif. Akibatnya, banyak regulasi yang hanya berfungsi sebagai solusi sementara dan belum mampu menjangkau secara komprehensif berbagai bentuk kejahatan digital yang terus mengalami evolusi, seperti serangan ransomware yang memanfaatkan kecerdasan buatan, penggunaan teknologi deepfake untuk tujuan penipuan dan manipulasi informasi, maupun serangan terhadap rantai pasok digital (*supply-chain attacks*) yang dapat mengancam infrastruktur strategis dan layanan publik. Situasi tersebut menunjukkan adanya kesenjangan antara perkembangan teknologi dengan kemampuan hukum untuk mengaturnya secara efektif. Oleh karena itu, muncul persoalan mendasar yang perlu dikaji secara kritis, yaitu sejauh mana hukum pidana dapat menjalankan fungsinya sebagai instrumen pengendalian sosial yang efektif dalam ruang digital yang tidak mengenal batas wilayah, memiliki tingkat keterhubungan yang sangat tinggi, serta terus berubah mengikuti dinamika perkembangan teknologi

[1] Setyo Bimo Anggoro et al., "Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan Di Era Digital Di Negara Maju Dan Berkembang," *Syntax Literate: Jurnal Ilmiah Indonesia* 9, no. 10 (2024): 5381–91, https://doi.org/10.36418/syntax-literate.v9i10.16452.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

global.[2]

Di Indonesia, kerangka hukum utama untuk menangani kejahatan siber berpusat pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah mengalami dua kali amandemen terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Amandemen kedua ini bertujuan memperkuat perlindungan anak di ruang digital, mengatur kontrak elektronik internasional, serta menyesuaikan beberapa ketentuan dengan Kitab Undang-Undang Hukum Pidana (KUHP) baru yang mulai berlaku secara penuh pada 2026. Selain itu, terdapat Undang-Undang Perlindungan Data Pribadi (UU PDP) dan berbagai peraturan turunan dari Badan Siber dan Sandi Negara (BSSN) terkait manajemen insiden siber.[3]

Secara kritis, regulasi ini masih menuai kritik tajam. Beberapa pasal di UU ITE dinilai overbroad dan rentan disalahgunakan untuk membatasi kebebasan berekspresi, seperti ketentuan tentang pencemaran nama baik, ujaran kebencian, dan penyebaran berita bohong yang dapat menimbulkan "kerusuhan". Putusan Mahkamah Konstitusi baru-baru ini pun menegaskan perlunya interpretasi ketat agar ketentuan tersebut tidak mencakup ruang digital secara berlebihan. Pada faktanya di lapangan, penegakan hukum masih menghadapi kendala struktural seperti keterbatasan sumber daya manusia yang menguasai forensik digital, infrastruktur investigasi yang belum memadai, serta kesulitan menangani kasus lintas yurisdiksi.[4] Akibatnya, meski kasus cybercrime terus meningkat terutama penipuan daring dan pembobolan data tingkat keberhasilan penanganan dan pemulihan kerugian korban masih rendah. Ini menunjukkan adanya kesenjangan antara norma di atas kertas dan realitas implementasi.

Sementara di Amerika Serikat, pengaturan kejahatan siber lebih tersebar dan matang secara historis. *Computer Fraud and Abuse Act* (CFAA) tahun 1986[5] (dengan berbagai amandemen) menjadi tulang punggung, didukung oleh undang-undang lain seperti *Digital Millennium Copyright Act* (DMCA)[6] dan berbagai ketentuan di level federal maupun negara bagian. Putusan Mahkamah Agung dalam kasus Van Buren v. United States (2021) sempat

---

[2] Elvan Maulana Rif'at and Timbul Dompak, "Hak Asasi Manusia Di Era Digital: Tantangan Dan Peluang Dalam Mengatasi Kejahatan Siber," *Jurnal Ilmu Multidisiplin* 3, no. 1 (2025): 86–98, https://doi.org/10.53935/jim.v3.i1.30.

[3] Winnie Rolindrawan, Nico Mooduto, and Agung Kurniawan Sihombing, "Indonesia - Cybersecurity Laws and Regulations 2026," November 2025, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/indonesia/.

[4] Benjamin A Soullier, "Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren," *Federal Communications Law Journal* 76, no. 2 (2024): 239–69, https://www.fclj.org/wp-content/uploads/2024/01/76.2.2_Decriminalizing-Trivial-Computer-Use-The-Need-to-Narrow-the-Computer-Fraud-and-Abuse-Act-CFAA-After-Van-Buren.pdf.

[5] Cyber Centaurs Team, "Understanding the Computer Fraud and Abuse Act (CFAA)," February 2024, https://cybercentaurs.com/blog/understanding-the-computer-fraud-and-abuse-act-cfaa/.

[6] Zulkifli Rafli, "Examining Legal Precedents and Social Implications: Interplay Between Intellectual Property Rights and Digital Piracy in the Age of DMCA," *Moccasin Journal De Public Perspective* 1, no. 1 (2024): 6–15, https://doi.org/10.37899/mjdpp.v1i1.21.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

mempersempit interpretasi "*exceeds authorized access*", yang menunjukkan upaya judicial check terhadap penerapan CFAA yang terlalu luas. Sistem federal AS memungkinkan penanganan kasus lintas negara bagian dan internasional dengan lebih agresif, termasuk melalui kerja sama dengan lembaga seperti FBI dan DOJ.[7]

Struktur federal yang terdesentralisasi sering menimbulkan tumpang tindih kewenangan dan kesulitan koordinasi. CFAA juga dikritik karena potensi *overcriminalization*, di mana pelanggaran kecil (seperti melanggar terms of service) dapat dijerat dengan ancaman pidana berat. Selain itu, meski teknologi AS lebih maju, serangan siber terhadap infrastruktur kritis (seperti kasus ransomware Colonial Pipeline atau SolarWinds) mengungkap kerapuhan sistem dan ketergantungan berlebih pada sektor swasta. Pendekatan AS yang cenderung ofensif dan berorientasi pada keamanan nasional kadang menuai tuduhan melanggar privasi warga dan hak asasi di tingkat global. Perbandingan antara kedua negara mengungkap persamaan dan perbedaan yang signifikan. Keduanya menghadapi ancaman serupa berupa sifat transnasional cybercrime, namun pendekatannya berbeda.

Amerika Serikat memiliki pengalaman yang relatif lebih panjang dalam menghadapi dan mengatur kejahatan siber, didukung oleh regulasi yang lebih khusus, sistem kelembagaan yang lebih matang, serta kemampuan teknologi investigasi yang berkembang secara signifikan. Sementara itu, Indonesia masih berada dalam fase penguatan dan pembaruan kerangka hukum, terutama setelah perubahan Undang-Undang Informasi dan Transaksi Elektronik pada tahun 2024 serta implementasi Kitab Undang-Undang Hukum Pidana yang baru. Perbedaan tersebut menunjukkan bahwa kesenjangan antara kedua negara tidak hanya terletak pada aspek normatif berupa substansi peraturan perundang-undangan, tetapi juga mencakup kapasitas institusional, kesiapan sumber daya manusia, budaya hukum, dan kemampuan adaptasi terhadap perkembangan teknologi digital. Dalam perspektif yang lebih kritis, perbandingan antara kedua sistem hukum ini menjadi penting untuk menilai sejauh mana efektivitas masing-masing model dalam menghadapi ancaman kejahatan siber yang terus berkembang. Keberadaan regulasi yang lebih rinci dan kompleks di Amerika Serikat, misalnya, belum tentu secara otomatis menghasilkan perlindungan hukum yang lebih optimal, karena kompleksitas tersebut juga berpotensi menimbulkan persoalan koordinasi, tumpang tindih kewenangan, serta prosedur birokrasi yang lebih rumit dalam proses penegakan hukum.

Sebaliknya, Indonesia yang masih mengembangkan sistem hukumnya menghadapi tantangan untuk mempercepat modernisasi regulasi dan kelembagaan tanpa mengabaikan prinsip-prinsip negara hukum, kepastian hukum, proporsionalitas, serta perlindungan hak asasi manusia. Di tengah dinamika tersebut, berbagai persoalan strategis seperti yurisdiksi terhadap pelaku lintas negara, validitas dan pembuktian alat bukti elektronik,

[7] Karolus Charlaes Bego et al., "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan Di Dunia Maya (Desember 2024)," *Jurnal Kolaboratif Sains* 8, no. 1 (2025): 506–11, https://doi.org/10.56338/jks.v8i1.6740.

perlindungan data pribadi, efektivitas kerja sama internasional melalui mekanisme Mutual Legal Assistance (MLA), hingga pemanfaatan kecerdasan buatan baik sebagai instrumen kejahatan maupun sebagai sarana penegakan hukum, masih menjadi isu yang memerlukan perhatian serius. Tantangan-tantangan tersebut menunjukkan bahwa penanggulangan kejahatan siber tidak lagi dapat diselesaikan hanya melalui pendekatan hukum nasional semata, melainkan membutuhkan harmonisasi regulasi, penguatan kapasitas kelembagaan, serta kolaborasi internasional yang lebih efektif untuk menjawab kompleksitas ancaman di ruang digital yang semakin terintegrasi secara global.

Penelitian ini diharapkan tidak hanya memetakan persamaan dan perbedaan pengaturan hukum pidana, tetapi juga memberikan rekomendasi kebijakan yang lebih adaptif, berbasis bukti, dan berorientasi pada perlindungan korban serta pencegahan di tengah dinamika teknologi yang terus berubah dengan cepat. Berdasarkan uraian latar belakang diatas maka diangkatlah penelitian jurnal ini yang berjudul " **ANALISIS PERBANDINGAN PENGATURAN HUKUM PIDANA TERHADAP TINDAK KEJAHATAN SIBER DI INDONESIA DAN AMERIKA SERIKAT**"

Berdasarkan latar belakang mengenai meningkatnya kejahatan dunia maya, rumusan masalah dalam penelitian ini adalah bagaimana persamaan dan perbedaan pengaturan serta implementasi hukum pidana dalam penanggulangan cybercrime pada sistem hukum Indonesia dan Amerika Serikat. Selain itu, penelitian ini juga merumuskan permasalahan mengenai bagaimana peran institusi penegak hukum di kedua negara dalam menghadapi perkembangan kejahatan siber yang semakin kompleks, baik dari aspek regulasi, kewenangan, koordinasi antarinstansi, maupun efektivitas penegakan hukumnya.

B. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif yang berorientasi pada pengkajian dan analisis terhadap norma-norma hukum yang mengatur tindak pidana siber (cybercrime) dalam sistem hukum Indonesia dan Amerika Serikat. Fokus utama penelitian diarahkan pada penelaahan bahan hukum yang bersifat tertulis, meliputi peraturan perundang-undangan, regulasi pelaksana, serta berbagai pandangan dan doktrin hukum yang berkembang dalam kajian akademik. Melalui pendekatan ini, penelitian tidak hanya berupaya mengidentifikasi substansi pengaturan hukum yang berlaku, tetapi juga menelaah sejauh mana konstruksi norma tersebut mampu merespons perkembangan kejahatan siber yang terus mengalami transformasi seiring kemajuan teknologi informasi. Pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach), yaitu suatu pendekatan yang menitikberatkan pada penelaahan terhadap berbagai instrumen hukum yang mengatur kejahatan siber di Indonesia maupun Amerika Serikat.[8]

[8] Peter Mahmud Marzuki, *Penelitian Hukum*, Cetakan ke-2 (Jakarta: Kencana, 2008).

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

Analisis dilakukan dengan membandingkan struktur, ruang lingkup, serta substansi pengaturan yang terdapat dalam masing-masing rezim hukum guna menemukan titik persamaan dan perbedaan di antara keduanya. Selain memberikan gambaran mengenai karakteristik kebijakan hukum pidana yang dianut oleh kedua negara, pendekatan ini juga memungkinkan dilakukannya evaluasi kritis terhadap efektivitas pengaturan yang ada dalam menghadapi dinamika kejahatan siber yang bersifat lintas batas negara (transnational crime). Hasil kajian komparatif tersebut diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai keunggulan, kelemahan, serta peluang pengembangan kebijakan hukum pidana siber di Indonesia dengan mempertimbangkan pengalaman dan praktik hukum yang berkembang di Amerika Serikat.[9]

C. Hasil dan Pembahasan

1. Perbedaan dan persamaan pengaturan serta implementasi hukum pidana dalam penanggulangan kejahatan dunia maya (*cybercrime*) pada sistem hukum Indonesia dan Amerika Serikat

Perbandingan pengaturan dan implementasi hukum pidana dalam penanggulangan kejahatan dunia maya atau cybercrime antara Indonesia dan Amerika Serikat mengungkapkan dinamika yang kompleks di mana kedua negara berusaha menjawab ancaman digital yang semakin canggih, anonim, serta melintasi batas yurisdiksi, meskipun dengan pendekatan yang mencerminkan latar belakang filosofis, historis, dan struktural yang sangat berbeda. Di Indonesia, fondasi utama pengaturan cybercrime tertanam dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah mengalami perubahan signifikan melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir Undang-Undang Nomor 1 Tahun 2024 yang memperkuat aspek perlindungan anak melalui Pasal 16A, pengakuan bukti elektronik di Pasal 5, serta penyesuaian terhadap sertifikasi elektronik dan pelindungan sistem, yang selaras dengan Kitab Undang-Undang Hukum Pidana baru Nomor 1 Tahun 2023 yang memperluas asas wilayah, pelindungan, dan universal untuk menjangkau perbuatan di luar negeri yang berdampak di wilayah Indonesia, sementara di Amerika Serikat kerangka hukum lebih fragmentasi dan sektoral dengan Computer Fraud and Abuse Act sebagai pilar utama sejak 1986 yang telah diamandemen berkali-kali untuk menangani akses tidak sah, pencurian data, penipuan komputer, serta ancaman terhadap infrastruktur kritis, didukung oleh undang-undang pelengkap seperti Identity Theft Act dan regulasi privasi anak.[10]

Persamaan mendasar terletak pada pengakuan keduanya terhadap bukti

[9] Ibid.

[10] Aisha Saphira Pradyanda et al., "Analisis Perbandingan Hukum Pidana Atas Tindak Pidana Pornografi Terhadap Anak Antara Indonesia Dengan Amerika Serikat," *Indonesian Journal of Criminal Law* 5, no. 1 (2023): 18–36, https://doi.org/10.31960/ijocl.v5i1.2054.

elektronik sebagai alat bukti yang sah, kebutuhan yurisdiksi ekstra-teritorial untuk kejahatan transnasional, serta tujuan melindungi kepentingan umum, data pribadi, dan stabilitas sosial dari penyalahgunaan teknologi informasi, di mana kedua negara menghadapi tantangan serupa seperti kesulitan identifikasi pelaku anonim, pengumpulan bukti digital yang mudah dihapus, serta perlunya keseimbangan antara keamanan siber dengan hak kebebasan berekspresi dan privasi. Namun, perbedaan mencolok muncul dalam filosofi regulasi di mana Indonesia cenderung mengadopsi pendekatan terpusat dan umum melalui UU ITE yang sering kali memuat norma terbuka seperti larangan konten yang melanggar kesusilaan atau menimbulkan keonaran, yang berpotensi menimbulkan multitafsir dan kontroversi publik terkait pencemaran nama baik serta ujaran kebencian, mencerminkan prioritas ketertiban umum dan nilai-nilai Pancasila, sedangkan Amerika Serikat lebih mengandalkan pendekatan kasuistik dan berbasis hak properti yang memungkinkan adaptasi cepat melalui putusan pengadilan seperti kasus Van Buren yang membatasi interpretasi luas CFAA agar tidak menjerat aktivitas sehari-hari atau penelitian keamanan.[11]

Dalam implementasi, Indonesia masih bergulat dengan keterbatasan kapasitas forensik digital, koordinasi antarlembaga seperti Polri dan BSSN, serta hambatan kerja sama internasional akibat disparitas teknologi, sehingga penegakan kerap bersifat reaktif dan represif dengan risiko efek dingin terhadap demokrasi digital, di sisi lain Amerika Serikat memiliki keunggulan melalui lembaga khusus seperti FBI Cyber Division dengan sumber daya teknologi canggih, kolaborasi publik-swasta yang matang, serta mekanisme Mutual Legal Assistance yang lebih efektif, meskipun tetap dihadapkan pada kritik atas potensi pengawasan berlebihan yang mengancam privasi warga.[12]

Secara kritis, kedua sistem hukum pidana ini sering tertinggal dari laju inovasi kejahatan seperti ransomware, deepfake, dan serangan negara-sponsored, di mana Indonesia perlu lebih harmonisasi regulasi dengan KUHP baru untuk menghindari over-criminalization dan meningkatkan edukasi digital masyarakat, sementara Amerika Serikat harus terus menjaga keseimbangan agar tidak menjadi alat dominasi korporasi atau pemerintah federal, sehingga pembelajaran komparatif ini menekankan bahwa keberhasilan penanggulangan cybercrime bukan semata pada ketatnya sanksi pidana melainkan pada kemampuan sistem hukum untuk beradaptasi berkelanjutan, memperkuat kapasitas institusional, serta menjunjung prinsip hak asasi manusia di tengah transformasi digital yang tak terhindarkan.

[11] Sigid Suseno et al., "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences* 11, no. 1 (2025): 2439543, https://doi.org/10.1080/23311886.2024.2439543.

[12] Mohammad Fadil Imran, "Cyber Criminology: An Analysis of the Indonesian and the United States Police Perception," *International Journal of Cyber Criminology* 17, no. 2 (2023): 250–61, https://doi.org/10.5281/zenodo.4766715.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

2. Peran institusi penegak hukum dalam menghadapi perkembangan kejahatan siber di Indonesia dan Amerika Serikat

Perkembangan teknologi informasi telah mengubah karakter tindak pidana konvensional menjadi kejahatan berbasis digital yang memiliki jangkauan lintas batas negara. Oleh karena itu, institusi penegak hukum di Indonesia dan Amerika Serikat dituntut untuk tidak hanya menjalankan fungsi represif melalui penyidikan dan penuntutan, tetapi juga berperan dalam pencegahan, perlindungan data, pengawasan ruang siber, serta penguatan kerja sama internasional. Meskipun kedua negara memiliki tujuan yang sama dalam menanggulangi kejahatan siber, pendekatan kelembagaan dan kerangka regulasi yang digunakan menunjukkan perbedaan yang cukup signifikan.[13]

Di Indonesia, peran utama penegakan hukum terhadap kejahatan siber dijalankan oleh Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber Bareskrim Polri, yang bertugas melakukan penyelidikan, penyidikan, pelacakan digital, serta pengumpulan alat bukti elektronik. Peran tersebut diperkuat melalui perubahan terbaru Undang-Undang Informasi dan Transaksi Elektronik, yaitu Undang-Undang Nomor 1 Tahun 2024 yang menegaskan pentingnya perlindungan ruang digital yang aman, sehat, beretika, serta memberikan kepastian hukum terhadap penyalahgunaan teknologi informasi.

UU tersebut juga memperluas pengaturan mengenai tanggung jawab Penyelenggara Sistem Elektronik (PSE), perlindungan pengguna, serta pengakuan alat bukti elektronik dalam proses peradilan. Selain Polri, peran penegakan hukum juga melibatkan Kejaksaan Republik Indonesia sebagai institusi yang melakukan penuntutan terhadap pelaku kejahatan siber dan memastikan alat bukti digital dapat dipergunakan secara sah di persidangan. Penguatan posisi alat bukti elektronik menjadi aspek penting karena sebagian besar tindak pidana siber meninggalkan jejak digital yang memerlukan teknik forensik khusus.[14] Dalam konteks ini, informasi elektronik dan dokumen elektronik telah diakui sebagai alat bukti hukum yang sah berdasarkan ketentuan UU ITE. Peran lembaga penegak hukum Indonesia semakin relevan dengan berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional).

Dalam ketentuan tersebut ditegaskan bahwa hukum pidana Indonesia dapat diberlakukan terhadap tindak pidana di bidang teknologi informasi yang akibat hukumnya terjadi di wilayah Indonesia, sekalipun

[13] Indri Oktari, "Law Enforcement Policy in Handling Cyber Crime in Indonesia: Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Di Indonesia," *UPMI Proceeding Series* 2, no. 2 (2025): 89–97, https://upmiproceeding.my.id/index.php/ups/article/view/225.

[14] Stefano Caneppele, "Observing, Measuring, and Researching Cybercrime: A Scoping Review of Systematic Reviews Since 2010s," in *Understanding Crime Trends in a Hybrid Society*, ed. Marcelo F Aebi, Fernando Miró-Llinares, and Stefano Caneppele, SpringerBriefs in Criminology (Cham: Springer, 2025), 101–28, https://doi.org/10.1007/978-3-031-72387-2_5.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

perbuatan tersebut dilakukan dari luar negeri. Pengaturan ini memperkuat yurisdiksi nasional dalam menghadapi kejahatan siber yang bersifat transnasional, seperti peretasan sistem elektronik, pencurian data, penipuan daring, dan serangan terhadap infrastruktur digital nasional. Meskipun demikian, institusi penegak hukum di Indonesia masih menghadapi sejumlah tantangan. Pertama, kecepatan perkembangan teknologi sering kali lebih cepat dibandingkan perkembangan regulasi dan kemampuan aparat penegak hukum. Kedua, keterbatasan sumber daya manusia yang memiliki kompetensi digital forensik dan keamanan siber menyebabkan proses pembuktian sering menghadapi hambatan teknis. Ketiga, sebagian besar kejahatan siber dilakukan secara anonim dan melibatkan pelaku yang berada di yurisdiksi negara lain sehingga membutuhkan mekanisme kerja sama internasional yang efektif.[15]

Berbeda dengan Indonesia yang masih melakukan penguatan kelembagaan dan regulasi, Amerika Serikat telah memiliki sistem penegakan hukum siber yang lebih mapan dan terintegrasi. Peran utama dijalankan oleh Federal Bureau of Investigation (FBI), Department of Justice (DOJ), Cybersecurity and Infrastructure Security Agency (CISA), serta United States Secret Service. FBI memiliki Cyber Division yang secara khusus menangani penyelidikan tindak pidana siber, termasuk serangan ransomware, pencurian identitas, spionase siber, dan peretasan terhadap infrastruktur penting negara. Sementara itu, CISA berfokus pada perlindungan sistem informasi kritis dan peningkatan ketahanan siber nasional.[16]

Dalam aspek regulasi, Amerika Serikat masih menjadikan Computer Fraud and Abuse Act (CFAA) sebagai instrumen utama dalam penindakan akses ilegal terhadap sistem komputer. Namun, pendekatan penegakan hukumnya terus diperbarui melalui berbagai kebijakan keamanan siber nasional, termasuk penguatan perlindungan infrastruktur kritis, pengawasan ancaman siber berbasis kecerdasan buatan, dan peningkatan koordinasi antara sektor publik dan sektor privat. Penegakan hukum di Amerika Serikat juga didukung oleh laboratorium digital forensik yang modern, sistem intelijen siber yang terintegrasi, serta kemampuan investigasi lintas negara yang relatif lebih kuat dibandingkan banyak negara lain.

Walaupun memiliki kapasitas yang lebih maju, institusi penegak hukum Amerika Serikat tetap menghadapi tantangan yang kompleks. Serangan ransomware yang menargetkan lembaga pemerintah dan perusahaan strategis, kejahatan berbasis cryptocurrency, pencurian data berskala

[15] Enver Buçaj and Kenan Idrizaj, "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention," *Multidisciplinary Reviews* 8, no. 1 (2025): 2025024, https://doi.org/10.31893/multirev.2025024.

[16] Loso Judijanto, "Hukum Pidana Dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi," *Indonesian Research Journal on Education* 5, no. 1 (2025): 968–72, https://www.irje.org/irje/article/view/2114.

besar, serta ancaman dari kelompok peretas yang didukung negara asing menjadi persoalan yang terus berkembang. Selain itu, terdapat perdebatan mengenai batas kewenangan aparat dalam mengakses data digital karena harus tetap memperhatikan perlindungan hak privasi dan kebebasan sipil warga negara. Jika dibandingkan, peran institusi penegak hukum di Indonesia dan Amerika Serikat memiliki kesamaan dalam hal melakukan penyelidikan, penindakan, pengumpulan bukti elektronik, serta pengembangan kerja sama internasional untuk menghadapi kejahatan siber yang bersifat lintas negara. Namun, Amerika Serikat cenderung lebih unggul dalam aspek teknologi, sumber daya manusia, dan integrasi kelembagaan, sedangkan Indonesia masih berfokus pada penguatan regulasi, peningkatan kapasitas aparat, serta pembangunan sistem keamanan siber nasional yang lebih komprehensif. Maka dari itu, dapat disimpulkan bahwa institusi penegak hukum di Indonesia maupun Amerika Serikat memegang peranan sentral dalam menghadapi perkembangan kejahatan siber. Keberhasilan penanggulangan cybercrime tidak hanya bergantung pada keberadaan regulasi yang memadai, tetapi juga pada kemampuan aparat penegak hukum dalam menguasai teknologi digital, melakukan investigasi berbasis forensik elektronik, serta membangun kerja sama internasional yang efektif. Di era digital saat ini, penegakan hukum siber harus dipandang sebagai upaya multidimensional yang menggabungkan aspek hukum, teknologi, keamanan nasional, dan perlindungan hak-hak masyarakat.

D. Penutup

Berdasarkan perbandingan sistem hukum Indonesia dan Amerika Serikat dalam penanggulangan kejahatan siber, dapat disimpulkan bahwa kedua negara memiliki tujuan yang sama, yaitu memberikan perlindungan terhadap masyarakat, data pribadi, sistem elektronik, dan kepentingan negara dari ancaman kejahatan berbasis teknologi informasi. Persamaan tersebut terlihat dari pengakuan terhadap alat bukti elektronik sebagai alat bukti yang sah, penerapan yurisdiksi terhadap tindak pidana siber yang bersifat lintas negara, serta penggunaan instrumen hukum pidana sebagai sarana utama untuk menindak pelaku kejahatan digital.

Dengan adanya persamaan tujuan tersebut diwujudkan melalui model regulasi dan implementasi yang berbeda sesuai dengan karakter sistem hukum masing-masing negara. Indonesia mengembangkan pengaturan cybercrime melalui pendekatan yang relatif terpusat dengan menjadikan Undang-Undang Informasi dan Transaksi Elektronik serta KUHP Nasional sebagai landasan utama penegakan hukum. Sebaliknya, Amerika Serikat menerapkan pendekatan yang lebih sektoral dan dinamis melalui berbagai regulasi federal yang didukung oleh perkembangan preseden peradilan. Perbedaan ini menunjukkan bahwa efektivitas penanggulangan kejahatan siber tidak hanya ditentukan oleh keberadaan norma hukum, melainkan juga oleh kemampuan sistem hukum untuk menyesuaikan diri dengan perubahan

teknologi yang berlangsung sangat cepat.

Dalam praktiknya, Amerika Serikat memiliki keunggulan pada aspek kapasitas kelembagaan, integrasi teknologi, sumber daya manusia, dan jaringan kerja sama internasional, sedangkan Indonesia masih menghadapi tantangan berupa keterbatasan kapasitas forensik digital, tumpang tindih kewenangan antarinstansi, serta kesenjangan antara perkembangan teknologi dan kemampuan penegakan hukum. Kajian ini juga menunjukkan bahwa peran institusi penegak hukum merupakan faktor yang menentukan keberhasilan implementasi hukum pidana di ruang siber. Keberadaan regulasi yang komprehensif tidak akan memberikan hasil optimal apabila tidak didukung oleh aparat yang memiliki kompetensi digital, infrastruktur teknologi yang memadai, serta mekanisme koordinasi yang efektif. Dalam konteks Indonesia, Direktorat Tindak Pidana Siber Polri, Kejaksaan, dan lembaga terkait telah menunjukkan peran yang semakin penting dalam menghadapi berbagai bentuk kejahatan digital.

Akan tetapi, efektivitas penegakan hukum masih memerlukan penguatan kapasitas kelembagaan dan peningkatan kemampuan teknis yang berkelanjutan. Sementara itu, pengalaman Amerika Serikat menunjukkan bahwa keberhasilan penanggulangan cybercrime lebih banyak ditopang oleh sinergi antara lembaga penegak hukum, sektor swasta, komunitas keamanan siber, dan kerja sama internasional. Dalam hal ini, dapat dinyatakan bahwa tantangan terbesar yang dihadapi kedua negara bukan lagi sekadar penegakan hukum terhadap bentuk-bentuk kejahatan siber konvensional, melainkan kemampuan merespons ancaman baru seperti ransomware, kecerdasan buatan yang disalahgunakan, deepfake, pencurian aset digital, serta serangan terhadap infrastruktur kritis negara. Oleh karena itu, efektivitas hukum pidana di era digital harus diukur tidak hanya dari banyaknya pelaku yang berhasil dihukum, tetapi juga dari kemampuan negara membangun sistem keamanan siber yang adaptif, preventif, dan tetap menghormati prinsip hak asasi manusia, privasi, serta kepastian hukum.

Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah
Volume 7 Nomor 4 Juli 2026
ISSN (Online): 2714-6917
Halaman 4067-4079

DAFTAR PUSTAKA

Buku

Marzuki, Peter Mahmud. *Penelitian Hukum*. Cetakan ke-2. Jakarta: Kencana, 2008.

Jurnal

Anggoro, Setyo Bimo, Arief Amrullah, Fanny Tanuwijaya, and Bayu Dwi Anggono. "Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan Di Era Digital Di Negara Maju Dan Berkembang." *Syntax Literate: Jurnal Ilmiah Indonesia* 9, no. 10 (2024): 5381–91. https://doi.org/10.36418/syntax-literate.v9i10.16452.

Bego, Karolus Charlaes, Fajar Rahmat Aziz, Riadi Asra Rahmad, Sunarto, and Heri Budianto. "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan Di Dunia Maya (Desember 2024)." *Jurnal Kolaboratif Sains* 8, no. 1 (2025): 506–11. https://doi.org/10.56338/jks.v8i1.6740.

Buçaj, Enver, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention." *Multidisciplinary Reviews* 8, no. 1 (2025): 2025024. https://doi.org/10.31893/multirev.2025024.

Caneppele, Stefano. "Observing, Measuring, and Researching Cybercrime: A Scoping Review of Systematic Reviews Since 2010s." In *Understanding Crime Trends in a Hybrid Society*, edited by Marcelo F Aebi, Fernando Miró-Llinares, and Stefano Caneppele, 101–28. SpringerBriefs in Criminology. Cham: Springer, 2025. https://doi.org/10.1007/978-3-031-72387-2_5.

Imran, Mohammad Fadil. "Cyber Criminology: An Analysis of the Indonesian and the United States Police Perception." *International Journal of Cyber Criminology* 17, no. 2 (2023): 250–61. https://doi.org/10.5281/zenodo.4766715.

Judijanto, Loso. "Hukum Pidana Dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi." *Indonesian Research Journal on Education* 5, no. 1 (2025): 968–72. https://www.irje.org/irje/article/view/2114.

Oktari, Indri. "Law Enforcement Policy in Handling Cyber Crime in Indonesia: Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Di Indonesia." *UPMI Proceeding Series* 2, no. 2 (2025): 89–97. https://upmiproceeding.my.id/index.php/ups/article/view/225.

Pradyanda, Aisha Saphira, Angelique Martahan Sibuea, Novela Julia Khosyi, and Shafa Haura Wijaya. "Analisis Perbandingan Hukum Pidana Atas Tindak Pidana Pornografi Terhadap Anak Antara Indonesia Dengan Amerika Serikat." *Indonesian Journal of Criminal Law* 5, no. 1 (2023): 18–36. https://doi.org/10.31960/ijocl.v5i1.2054.

Rafli, Zulkifli. "Examining Legal Precedents and Social Implications: Interplay Between Intellectual Property Rights and Digital Piracy in the Age of DMCA." *Moccasin Journal De Public Perspective* 1, no. 1 (2024): 6–15. https://doi.org/10.37899/mjdpp.v1i1.21.

Rif'at, Elvan Maulana, and Timbul Dompak. "Hak Asasi Manusia Di Era Digital: Tantangan Dan Peluang Dalam Mengatasi Kejahatan Siber." *Jurnal Ilmu Multidisiplin* 3, no. 1 (2025): 86–98. https://doi.org/10.53935/jim.v3.i1.30.

Soullier, Benjamin A. "Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After Van Buren." *Federal Communications Law Journal* 76, no. 2 (2024): 239–69. https://www.fclj.org/wp-content/uploads/2024/01/76.2.2_Decriminalizing-Trivial-Computer-Use-The-Need-to-Narrow-the-Computer-Fraud-and-Abuse-Act-CFAA-After-Van-Buren.pdf.

Suseno, Sigid, Ahmad M Ramli, Ranti Fauza Mayana, Tasya Safiranita, and Bernadette Aurellia Nathania Tiarma. "Cybercrime in the New Criminal Code in Indonesia." *Cogent Social Sciences* 11, no. 1 (2025): 2439543. https://doi.org/10.1080/23311886.2024.2439543.

Website

Cyber Centaurs Team. "Understanding the Computer Fraud and Abuse Act (CFAA)," February 2024. https://cybercentaurs.com/blog/understanding-the-computer-fraud-and-abuse-act-cfaa/.

Rolindrawan, Winnie, Nico Mooduto, and Agung Kurniawan Sihombing. "Indonesia - Cybersecurity Laws and Regulations 2026," November 2025. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/indonesia/.