Journal Terekam Jejak (JTJ), Copyright © 2025
Vol. 3, Num. 3, 2025
https://journal.terekamjejak.com/index.php/jtj/index
Author: **Bunga Anggreini**

Penguatan Hukum Pidana Indonesia dalam Menghadapi Kejahatan Siber Era Digital

ABSTRACT

The rapid development of information technology in the digital era has given rise to a new form of crime known as cybercrime. This phenomenon poses a major challenge to Indonesia's criminal law system, which is still heavily influenced by the colonial-era Criminal Code (KUHP). This article aims to conduct an in-depth analysis of the Indonesian criminal law's response to cybercrime. The focus includes evaluating regulatory developments, the effectiveness of law enforcement, and the absolute urgency of criminal law reform. This study employs a normative juridical method, supported by statutory (statute approach), conceptual (conceptual approach), and comparative (comparative approach) approaches. The findings show an increasing trend of cybercrime in Indonesia, ranging from online fraud and hacking to the spread of hoaxes and hate speech. Although the Electronic Information and Transactions Law (ITE Law) and its implementing regulations provide a legal framework, substantial weaknesses remain in terms of legal certainty, human rights protection (HAM), and the technical capacity of law enforcement agencies. Therefore, criminal law reform is urgently needed, focusing not only on penal sanctions but also on prevention, strengthening digital infrastructure, and close international cooperation.

Keyword: criminal law, cybercrime, ITE Law, legal reform

ABSTRAK

Perkembangan pesat teknologi informasi di era digital telah memunculkan suatu bentuk kejahatan baru yang dikenal sebagai kejahatan siber (cybercrime). Fenomena ini menjadi tantangan besar bagi sistem hukum pidana Indonesia, yang masih sangat dipengaruhi oleh Kitab Undang-Undang Hukum Pidana (KUHP) warisan kolonial. Artikel ini bertujuan untuk melakukan analisis mendalam mengenai respons hukum pidana Indonesia terhadap kejahatan siber. Fokusnya mencakup evaluasi perkembangan regulasi, tingkat efektivitas penegakan hukum, dan urgensi mutlak untuk melakukan pembaruan hukum pidana. Penelitian ini menggunakan metode yuridis normatif, didukung oleh pendekatan perundang- undangan (statute approach), konseptual (conceptual approach), dan komparatif (comparative approach). Hasil kajian menunjukkan adanya tren peningkatan kejahatan siber di Indonesia, mulai dari penipuan daring, peretasan, hingga penyebaran hoaks dan ujaran kebencian. Meskipun telah ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan sejumlah peraturan pelaksana, masih ditemukan kelemahan substansial dalam aspek kepastian hukum, perlindungan hak asasi manusia (HAM), dan kapasitas teknis aparat penegak hukum. Oleh karena itu, reformasi hukum pidana sangat mendesak, dan tidak hanya

harus berfokus pada aspek pemidanaan, tetapi juga pada langkah pencegahan, penguatan infrastruktur digital, dan kerja sama internasional yang erat.

Kata Kunci: hukum pidana, kejahatan siber, UU ITE, reformasi hukum

PENDAHULUAN

"Kejahatan siber di Indonesia semakin meningkat, mulai dari penipuan daring, peretasan, hingga penyebaran ujaran kebencian. Walaupun telah ada UU ITE, regulasi tersebut masih menimbulkan kontroversi karena multitafsir. Oleh karena itu, diperlukan analisis hukum pidana yang lebih komprehensif dan reformasi hukum yang berkeadilan (Hasan, 2025a)."

Era digital telah membawa transformasi fundamental dalam kehidupan masyarakat. Internet kini tidak hanya berperan sebagai sarana komunikasi, tetapi telah menjadi ruang utama untuk aktivitas kerja, pembelajaran, bisnis, dan interaksi sosial. Sayangnya, kemajuan ini juga diiringi dengan lahirnya kejahatan siber, yang sulit dikendalikan karena sifatnya yang lintas batas (transnasional), anonim, dan memanfaatkan teknologi canggih.

Indonesia menghadapi ancaman siber yang serius. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2021 mencatat lebih dari 1,6 miliar serangan siber terjadi sepanjang tahun tersebut. Bentuk kejahatannya bervariasi, meliputi pencurian data pribadi, berbagai modus penipuan berbasis aplikasi, hingga serangan ransomware yang menimbulkan kerugian besar di sektor keuangan. Dampaknya meluas tidak hanya pada sektor ekonomi, tetapi juga memunculkan isu-isu sosial seperti maraknya penyebaran ujaran kebencian, fitnah, hoaks, dan pornografi anak.

Di sisi lain, sistem hukum pidana nasional Indonesia belum sepenuhnya siap menghadapi tantangan ini. KUHP, sebagai fondasi hukum pidana, tidak memiliki pasal khusus yang mengatur kejahatan yang bersifat digital. Walaupun UU ITE menjadi payung hukum utama, regulasi ini seringkali menimbulkan kontroversi karena interpretasinya yang multitafsir dan rawan disalahgunakan, bahkan memicu kriminalisasi warga negara. Oleh karena itu, diperlukan analisis

komprehensif terhadap respons hukum pidana dan sebuah reformasi hukum yang berkeadilan. Analisis komprehensif itu antara lain:

1. Regulasi Hukum Pidana

"Sistem hukum pidana Indonesia pada dasarnya masih berlandaskan KUHP warisan kolonial. Hal ini menyebabkan keterbatasan dalam merespons bentuk-bentuk kejahatan baru, termasuk kejahatan siber. Menurut Hasan (2025a), asas legalitas dan asas keadilan merupakan prinsip mendasar yang harus diperkuat dalam pembaruan hukum pidana."

2. Penegakan Hukum

"Penegakan hukum dalam kasus kejahatan siber memerlukan sinergi antara kepolisian,kejaksaan, pengadilan, dan advokat. Hal ini sejalan dengan konsep sistem peradilan pidana yang menekankan integrasi antar-subsistem penegak hukum (Hasan, 2025b)."

Di tengah hiruk pikuk kemajuan teknologi informasi yang tak terbendung, kita menyaksikan sebuah paradoks yang menarik sekaligus mengkhawatirkan. Era digital, yang seharusnya membawa kemudahan dan konektivitas tanpa batas, ternyata juga melahirkan bayang-bayang gelap berupa bentuk-bentuk kejahatan baru yang kita kenal sebagai kejahatan siber.

Fenomena ini bukan sekadar isu teknis, melainkan sebuah tantangan besar yang menguji fondasi sistem hukum pidana Indonesia. Bayangkan saja, sistem hukum kita yang masih banyak berlandaskan pada Kitab Undang-Undang Hukum Pidana (KUHP) warisan kolonial, kini harus berhadapan dengan kejahatan yang sifatnya virtual, lintas batas, dan seringkali anonim.

Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan sejumlah peraturan turunannya telah hadir sebagai respons awal, kita tidak bisa memungkiri bahwa masih banyak celah dan kelemahan. Aspek kepastian hukum seringkali menjadi pertanyaan, perlindungan hak asasi manusia kerap terabaikan, dan kapasitas aparat penegak hukum masih perlu ditingkatkan. Oleh karena itu, reformasi hukum pidana bukan lagi pilihan, melainkan sebuah

keharusan. Reformasi ini tidak hanya berfokus pada aspek pemidanaan semata, tetapi juga pada upaya pencegahan, penguatan infrastruktur digital, dan kerja sama internasional yang solid.

Perkembangan teknologi digital telah membawa perubahan besar dalam kehidupan masyarakat. Internet kini tidak hanya menjadi sarana komunikasi, tetapi juga ruang untuk bekerja, belajar, berbisnis, bahkan bersosialisasi. Namun, kemajuan ini diiringi dengan lahirnya kejahatan siber yang sulit dikendalikan karena sifatnya lintas batas, anonim, dan menggunakan teknologi canggih. Indonesia menghadapi situasi yang cukup serius. Laporan BSSN tahun 2021 mencatat lebih dari 1,6 miliar serangan siber sepanjang tahun. Bentuknya bervariasi, mulai dari pencurian data pribadi, penipuan berbasis aplikasi, hingga serangan ransomware yang merugikan sektor keuangan. Tidak hanya berdampak ekonomi, kejahatan siber juga memunculkan masalah sosial seperti penyebaran ujaran kebencian, fitnah, hoaks, dan pornografi anak.

3. Perlindungan HAM

"Kejahatan siber seringkali menyangkut pelanggaran hak asasi manusia, terutama hak atas privasi dan kebebasan berekspresi. Dalam konteks ini, bantuan hukum menjadi instrumen penting untuk menjamin kesetaraan warga negara di depan hukum (Hasan, 2025c)."

4. Dimensi Sosial

"Fenomena penyimpangan di ruang digital dapat dipandang sebagai bagian dari penyimpangan sosial, yang membutuhkan mekanisme pengendalian sosial baru agar masyarakat terlindungi (Hasan, 2024)."

5. Risiko Korupsi dalam Tata Kelola Digital

"Selain itu, pengelolaan teknologi informasi publik juga berisiko disalahgunakan untuk praktik korupsi. Oleh karena itu, integrasi pendidikan antikorupsi perlu dikedepankan untuk membangun budaya hukum yang bersih dan transparan (Hasan, 2025d)." Perkembangan teknologi digital telah membawa perubahan besar dalam kehidupan masyarakat. Internet kini tidak

hanya menjadi sarana komunikasi, tetapi juga ruang untuk bekerja, belajar, berbisnis, bahkan bersosialisasi. Namun, kemajuan ini diiringi dengan lahirnya kejahatan siber yang sulit dikendalikan karena sifatnya lintas batas, anonim, dan menggunakan teknologi canggih.

Indonesia menghadapi situasi yang cukup serius. Laporan BSSN tahun 2021 mencatat lebih dari 1,6 miliar serangan siber sepanjang tahun. Bentuknya bervariasi, mulai dari pencurian data pribadi, penipuan berbasis aplikasi, hingga serangan ransomware yang merugikan sektor keuangan. Tidak hanya berdampak ekonomi, kejahatan siber juga memunculkan masalah sosial seperti penyebaran ujaran kebencian, fitnah, hoaks, dan pornografi anak.

Sementara itu, sistem hukum pidana Indonesia masih belum siap sepenuhnya menghadapi tantangan ini. KUHP sebagai dasar hukum pidana nasional tidak memiliki pasal yang secara khusus mengatur kejahatan digital. UU ITE memang menjadi payung hukum utama, tetapi beberapa pasalnya sering menimbulkan kontroversi karena multitafsir dan rawan disalahgunakan.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif. Penelitian ini menelaah secara mendalam berbagai aturan hukum positif, asas hukum, doktrin hukum, dan putusan pengadilan yang relevan dengan tindak pidana siber. Tiga pendekatan utama digunakan dalam penelitian ini:

1. Pendekatan Perundang-undangan (Statute Approach): Menelaah secara spesifik KUHP, UU ITE, Peraturan Pemerintah Nomor 71 Tahun 2019 (PP 71/2019), serta peraturan BSSN.
2. Pendekatan Konseptual (Conceptual Approach): Mengkaji berbagai teori hukum pidana, asas legalitas, dan konsep perlindungan hak asasi manusia (HAM).

3. Pendekatan Komparatif (Comparative Approach): Membandingkan regulasi cybercrime di Indonesia dengan kerangka hukum negara lain, seperti Amerika Serikat dan Uni Eropa.

Bahan hukum yang digunakan antara lain:

- Primer: peraturan perundang-undangan & putusan pengadilan.
- Sekunder: buku teks & artikel jurnal hukum.
- Tersier: laporan resmi dari BSSN, Kominfo, serta laporan internasional seperti Interpol.

HASIL DAN PEMBAHASAN

Perkembangan Kejahatan Siber di Indonesia

Kejahatan siber terus berkembang seiring dengan jumlah pengguna internet di Indonesia yang telah melampaui 210 juta orang. Tren peningkatan kejahatan ini ditandai oleh kompleksitas dan kerugian yang ditimbulkan. Beberapa kasus menonjol yang menunjukkan kerentanan siber nasional meliputi:

- Penipuan daring yang terjadi melalui media sosial dan e-commerce.
- Peretasan (hacking) terhadap sistem perbankan dan instansi pemerintah.
- Pencurian data pribadi yang kemudian diperjualbelikan secara ilegal di dark web.
- Serangan Ransomware yang melumpuhkan layanan publik.
- Penyebaran hoaks dan ujaran kebencian yang memiliki potensi kuat untuk mengganggu stabilitas sosial.

Kasus Bjorka pada tahun 2022 secara khusus mempertegas bahwa Indonesia menghadapi ancaman serius dalam tata kelola data pribadi. Kasus ini

juga menyoroti lemahnya koordinasi serta perbedaan pandangan di antara lembaga penegak hukum dan penyelenggara sistem elektronik.

Regulasi Hukum Pidana yang Berlaku

Regulasi yang berlaku saat ini menunjukkan bahwa hukum pidana Indonesia masih belum solid dalam menghadapi cybercrime.

- KUHP: sebagai dasar hukum pidana nasional, KUHP belum mengakomodasi perkembangan cybercrime.
- UU ITE (UU No. 11/2008 jo. UU No. 19/2016): menjadi dasar utama, namun beberapa pasalnya, seperti Pasal 27 ayat (3) tentang pencemaran nama baik, sering diperdebatkan.

Meskipun berbagai kendala masih dihadapi, terdapat beberapa langkah maju dalam upaya penegakan hukum dan perlindungan terhadap kejahatan siber di Indonesia. Salah satunya adalah dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menjadi tonggak penting dalam melindungi hak privasi warga negara di era digital. Kehadiran undang-undang ini menunjukkan komitmen pemerintah untuk memperkuat regulasi terkait pengelolaan dan keamanan data pribadi, meskipun implementasinya masih berada pada tahap awal dan memerlukan pengawasan yang konsisten.

Selain itu, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan landasan hukum bagi penyelenggara sistem elektronik di Indonesia. Namun, peraturan ini lebih menekankan pada aspek administratif dan teknis penyelenggaraan sistem, sehingga belum sepenuhnya menyentuh dimensi pidana dalam penegakan hukum siber.

Langkah lainnya adalah diterbitkannya peraturan Badan Siber dan Sandi Negara (BSSN) yang berfokus pada peningkatan keamanan sistem informasi nasional. Meskipun secara substansi telah mengatur kerangka kerja keamanan siber, implementasi di lapangan masih dinilai lemah karena keterbatasan koordinasi antar instansi dan kurangnya kesiapan sumber daya.

Secara keseluruhan, keberadaan berbagai regulasi tersebut menandai kemajuan dalam sistem hukum siber di Indonesia, meskipun masih dibutuhkan penguatan pada aspek pelaksanaan agar tujuan perlindungan dan keamanan digital dapat tercapai secara optimal.

Kelemahan Penegakan Hukum

Praktik penegakan hukum pidana terhadap kejahatan siber di Indonesia menghadapi berbagai persoalan yang cukup kompleks. Salah satu masalah utama terletak pada pasal-pasal dalam UU ITE yang seringkali bersifat multitafsir, sehingga menimbulkan ketidakpastian hukum. Hal ini dapat dilihat dari kasus Baiq Nuril pada tahun 2018, di mana penerapan pasal-pasal UU ITE menimbulkan perdebatan mengenai batas antara kebebasan berekspresi dan pelanggaran hukum.

Selain itu, keterbatasan sumber daya manusia (SDM) aparat penegak hukum juga menjadi hambatan serius, terutama dalam bidang forensik digital. Kasus peretasan yang dilakukan oleh Bjorka menjadi salah satu bukti nyata lemahnya kemampuan investigasi terhadap serangan siber di Indonesia. Kondisi ini menunjukkan perlunya peningkatan kapasitas dan pelatihan bagi aparat dalam menangani kejahatan berbasis teknologi.

Masalah lain muncul dari kurangnya koordinasi antar lembaga yang berwenang, seperti Kepolisian Republik Indonesia (Polri), Kementerian Komunikasi dan Informatika (Kominfo), serta Badan Siber dan Sandi Negara (BSSN). Ketiga lembaga tersebut sering kali menjalankan fungsi yang tumpang

tindih dan belum terintegrasi secara efektif, sehingga penanganan kasus siber menjadi kurang efisien.

Selain itu, aspek Hak Asasi Manusia (HAM) juga kerap terabaikan dalam proses penegakan hukum. UU ITE sering digunakan sebagai alat untuk membungkam kritik masyarakat terhadap pemerintah. Berdasarkan laporan SAFEnet tahun 2021, tercatat lebih dari 70 kasus kriminalisasi warga yang disebabkan oleh penerapan pasal-pasal multitafsir dalam UU ITE. Fakta ini menegaskan perlunya reformasi dalam penegakan hukum siber agar tidak hanya berorientasi pada keamanan, tetapi juga tetap menjunjung tinggi prinsip keadilan dan perlindungan hak asasi manusia.

Strategi Pembaruan Hukum Pidana

Untuk mengatasi tantangan kompleks ini, strategi pembaruan hukum pidana yang ideal harus dilaksanakan secara terstruktur:

1. Revisi KUHP dan UU ITE: KUHP perlu direvisi untuk memasukkan pasal-pasal khusus mengenai cybercrime. UU ITE juga harus direformasi agar menjadi lebih jelas, tidak multitafsir, dan sejalan dengan prinsip perlindungan HAM.
2. Penguatan Kapasitas Aparat: Diperlukan peningkatan kualitas SDM aparat melalui pelatihan khusus dan penyediaan teknologi forensik digital canggih. Hal ini sejalan dengan konsep sistem peradilan pidana yang mengedepankan sinergi antar-subsistem penegak hukum (kepolisian, kejaksaan, pengadilan, advokat).
3. Kerja Sama Internasional: Mengingat sifat kejahatan siber yang transnasional, kerja sama internasional dalam melacak kejahatan menjadi mutlak. Pembelajaran dapat diambil dari regulasi negara lain seperti Computer Fraud and Abuse Act (Amerika Serikat) dan General Data Protection Regulation (Uni Eropa).
4. Pendekatan Non-Penal: Selain pemidanaan, langkah pencegahan harus diintensifkan, termasuk melalui literasi digital, kampanye etika

bermedia sosial, dan penguatan sistem keamanan siber nasional. Pendekatan ini juga mencakup pembangunan budaya hukum yang bersih melalui integrasi pendidikan antikorupsi, mengingat adanya risiko korupsi dalam tata kelola digital publik.

KESIMPULAN

Dengan demikian, strategi reformasi hukum pidana Indonesia harus memperhatikan aspek asas legalitas, perlindungan HAM, dan pendidikan antikorupsi sebagaimana ditegaskan oleh Hasan (2025a; 2025d). Kejahatan siber merupakan ancaman serius yang semakin kompleks di era digital. Perkembangan kasus-kasus dari peretasan data pribadi, serangan *ransomware*, hingga penyalahgunaan pasal pencemaran nama baik dalam UU ITE menunjukkan bahwa kerangka regulasi dan penegakan hukum yang ada masih belum memadai. Berdasarkan pembahasan, dapat disimpulkan bahwa:

1. Peta Kejahatan Siber di Indonesia menunjukkan tren peningkatan yang signifikan, baik dalam jumlah maupun kompleksitas kasus, yang mengancam keamanan siber dan stabilitas sosial.
2. Regulasi Hukum Pidana masih berpusat pada UU ITE, tetapi substansinya sering multitafsir dan belum sepenuhnya sejalan dengan prinsip HAM.
3. Kelemahan Penegakan Hukum utama terletak pada keterbatasan kapasitas forensik digital aparat, lemahnya koordinasi antar lembaga, serta ketidakpastian hukum yang ditimbulkan oleh pasal-pasal multitafsir.
4. Strategi Reformasi Hukum Pidana yang Ideal meliputi revisi mendalam terhadap KUHP dan UU ITE, penguatan kapasitas aparat penegak hukum, peningkatan kerja sama internasional, dan pengedepanan pendekatan non-penal (literasi digital, etika bermedia sosial, dan perlindungan data pribadi).

Dengan langkah-langkah reformasi yang holistik, hukum pidana Indonesia akan menjadi lebih responsif terhadap tantangan dunia maya, sekaligus mampu menjaga keseimbangan penting antara keamanan siber dan perlindungan hak asasi manusia. Strategi ini harus berpegang teguh pada penguatan asas legalitas, perlindungan HAM, dan pembangunan budaya hukum yang bersih sebagaimana ditekankan oleh para ahli.

DAFTAR PUSTAKA

Arief, B. N. (2008). *Kebijakan legislatif dalam penanggulangan kejahatan dengan pidana penjara*. Pustaka Magister.

Atmasasmita, R. (2017). *Reformasi hukum pidana di Indonesia*. Mandar Maju.

Badan Siber dan Sandi Negara. (2021). *Laporan tahunan insiden siber di Indonesia*. BSSN.

Council of Europe. (2021). *Budapest convention on cybercrime: Implementation guide*. Strasbourg.

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

Hamzah, A. (2016). *Hukum pidana Indonesia*. Sinar Grafika.

Hasan, Z. (2024). *Sosiologi hukum masyarakat dan kebudayaan: Integrasi nilai sosial untuk pembangunan*. CV Alinea Edumedia.

Hasan, Z. (2025a). *Hukum pidana*. CV Alinea Edumedia.

Hasan, Z. (2025b). *Sistem peradilan pidana*. CV Alinea Edumedia.

Hasan, Z. (2025c). *Bantuan hukum*. UBL Press.

Hasan, Z. (2025d). *Pendidikan anti korupsi: Integrasi pencegahan tindak pidana korupsi di era 4.0*. UBL Press.

Interpol. (2020). *Cybercrime trends report*. Interpol.

Kementerian Komunikasi dan Informatika. (2022). *Statistik pengaduan konten internet*. Kominfo.

Moeljatno. (2015). *Asas-asas hukum pidana*. Rineka Cipta.

Muladi, & Arief, B. N. (2010). *Teori-teori dan kebijakan pidana*. Alumni.

Nasution, A. B. (2020). Problematika penegakan hukum tindak pidana siber di Indonesia. *Jurnal Hukum dan Pembangunan, 50*(3), 451–472.

Nugroho, Y. (2019). Urgensi pembaharuan hukum pidana dalam menghadapi kejahatan siber. *Jurnal Rechts Vinding, 8*(1), 1–18.

Peraturan Badan Siber dan Sandi Negara tentang Keamanan Siber.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP). (2022).

SAFEnet. (2021). *Digital rights report Indonesia*. SAFEnet.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.