

Penegakan Hukum Pidana terhadap Kejahatan Siber sebagai Dampak Perkembangan Teknologi Informasi

Nisrina Khairunisa Permana^{1*}, Anisa Ramadhanti², Sri Handayani³

^{1,2,3}Universitas Sriwijaya, Palembang, Sumsel, Indonesia

Informasi Artikel	Abstrak
Penulis Korespondensi: Nisrina Khairunisa Permana [nisrinanisa1357@gmail.com] Submission 2025-03-12 Review 2025-04-28 Accepted 2025-05-13 Publish 2025-05-15   This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.	Latar Belakang: Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam aktivitas ekonomi, sosial, dan pemerintahan. Transformasi digital yang semakin masif juga memunculkan bentuk-bentuk kejahatan baru yang memanfaatkan teknologi informasi, yang dikenal sebagai kejahatan siber (<i>cybercrime</i>). Kejahatan ini meliputi berbagai bentuk seperti penipuan online, peretasan sistem komputer, pencurian data pribadi, penyebaran konten ilegal, hingga serangan siber yang bersifat lintas negara. Kondisi tersebut menimbulkan tantangan serius bagi sistem penegakan hukum pidana karena karakteristik kejahatan siber yang kompleks, anonim, serta melampaui batas yurisdiksi negara. Tujuan Penelitian: untuk menganalisis efektivitas penegakan hukum pidana terhadap kejahatan siber di Indonesia serta mengidentifikasi berbagai kendala yang dihadapi dalam penanganannya. Metode Penelitian: Penelitian ini menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus melalui analisis terhadap berbagai regulasi terkait, khususnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016. Hasil Penelitian: menunjukkan bahwa meskipun Indonesia telah memiliki kerangka hukum yang relatif memadai untuk menanggulangi kejahatan siber, implementasi penegakan hukumnya masih menghadapi berbagai hambatan, antara lain keterbatasan kemampuan teknis aparat penegak hukum, kesulitan pembuktian digital, serta sifat transnasional dari kejahatan siber. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta kerja sama internasional yang lebih intensif untuk meningkatkan efektivitas penegakan hukum pidana terhadap kejahatan siber di era digital. Kata Kunci: cybercrime, penegakan hukum pidana, teknologi informasi, hukum siber, UU ITE Abstract Background: The development of information and communication technology has brought significant changes to various aspects of people's lives, including economic, social, and governmental activities. The increasingly massive digital transformation has also given rise to new forms of crime that utilize information technology, known as cybercrime. This crime includes various forms such as online fraud, computer system hacking, personal data theft, distribution of illegal content, and transnational cyber attacks. This condition poses a serious challenge to the criminal law enforcement system due to the complex, anonymous, and transcendent characteristics of cybercrime. Research Objective: To analyze the effectiveness of criminal law enforcement against cybercrime in Indonesia and identify various obstacles faced in handling it. Research Method: This research uses normative legal research with a statutory approach, a conceptual approach, and a case approach through an analysis of various related regulations, especially Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments through Law Number 19 of 2016. Research Results: shows that although Indonesia has a relatively adequate legal framework to combat cybercrime, the implementation of law enforcement still faces various obstacles, including limited technical capabilities of law enforcement officers, difficulties in digital evidence, and the transnational nature of cybercrime. Therefore, it is necessary to strengthen regulations, increase the capacity of law enforcement officers, and more intensive international cooperation to increase the effectiveness of criminal law enforcement against cybercrime in the digital era. Keywords: cybercrime, criminal law enforcement, information technology, cyber law, ITE Law

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar dalam kehidupan masyarakat modern. Internet, media sosial, serta berbagai platform digital telah menciptakan ruang interaksi baru yang memungkinkan pertukaran informasi secara cepat dan tanpa batas geografis. Transformasi digital tersebut memberikan berbagai manfaat bagi masyarakat, seperti kemudahan akses informasi, efisiensi dalam aktivitas ekonomi, serta peningkatan produktivitas di berbagai sektor kehidupan.

Namun demikian, perkembangan teknologi informasi juga membawa konsekuensi negatif berupa munculnya berbagai bentuk kejahatan baru yang memanfaatkan teknologi digital. Fenomena ini dikenal sebagai kejahatan siber (*cybercrime*), yaitu kejahatan yang dilakukan dengan menggunakan komputer, jaringan internet, atau sistem informasi sebagai sarana maupun sasaran kejahatan¹. Kejahatan siber dapat mencakup berbagai bentuk tindakan ilegal seperti penipuan online, pencurian identitas digital, penyebaran malware, peretasan sistem komputer, serta penyebaran konten ilegal melalui internet.

Seiring dengan meningkatnya penggunaan teknologi digital dalam berbagai aktivitas masyarakat, jumlah kasus kejahatan siber juga mengalami peningkatan yang signifikan. Berbagai laporan menunjukkan bahwa penipuan online, phishing, pencurian data pribadi, serta serangan ransomware menjadi ancaman yang semakin serius bagi keamanan digital masyarakat. Kondisi ini menunjukkan bahwa perkembangan teknologi informasi tidak hanya membawa manfaat, tetapi juga memunculkan risiko kejahatan baru yang lebih kompleks dibandingkan kejahatan konvensional.

Dalam konteks hukum pidana, kejahatan siber menimbulkan berbagai tantangan baru bagi aparat penegak hukum. Salah satu tantangan utama adalah sifat anonim dari pelaku kejahatan yang dapat menyembunyikan identitasnya melalui teknologi digital. Selain itu, kejahatan siber sering kali bersifat lintas negara sehingga menimbulkan persoalan yurisdiksi dan kerja sama internasional dalam proses penegakan hukum².

Untuk mengatasi permasalahan tersebut, Indonesia telah mengembangkan berbagai regulasi yang mengatur aktivitas di ruang digital. Salah satu regulasi utama yang menjadi dasar hukum dalam penanggulangan kejahatan siber adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Regulasi ini mengatur berbagai bentuk tindak pidana yang berkaitan dengan penggunaan teknologi informasi, termasuk akses ilegal terhadap sistem elektronik, manipulasi data elektronik, serta penyebaran informasi yang melanggar hukum.

Meskipun demikian, berbagai penelitian menunjukkan bahwa implementasi UU ITE dalam praktik penegakan hukum masih menghadapi berbagai kendala. Salah satu permasalahan yang sering muncul adalah keterbatasan kemampuan teknis aparat penegak hukum dalam menangani

¹ Widijowati, D. (2022). Legal complexity in dealing with cyber crime in Indonesia. *Research Horizon*, 2(4), 423–431.

² Banjarani, D. R., & Rahmadhani, A. N. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era digital di Indonesia. *Jurnal Yustisia*, 13(2), 145–158.

kejahatan yang berbasis teknologi informasi. Selain itu, perkembangan teknologi yang sangat cepat sering kali melampaui kemampuan regulasi hukum yang ada³.

Selain faktor teknis, kendala lain yang dihadapi dalam penegakan hukum terhadap kejahatan siber adalah masalah pembuktian dalam proses peradilan. Bukti digital memiliki karakteristik yang berbeda dengan alat bukti konvensional sehingga memerlukan metode investigasi khusus serta keahlian forensik digital. Tanpa dukungan teknologi dan sumber daya manusia yang memadai, proses pembuktian dalam perkara *cybercrime* dapat menjadi sangat kompleks⁴.

Meskipun penelitian mengenai kejahatan siber dan penegakan hukum pidana telah banyak dilakukan, sebagian besar kajian terdahulu masih berfokus pada aspek pengaturan normatif *cybercrime* dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta kompleksitas hukum dalam penanganan tindak pidana siber di Indonesia⁵. Penelitian lainnya lebih banyak membahas kedudukan alat bukti elektronik dalam proses pembuktian perkara *cybercrime* tanpa mengkaji secara mendalam efektivitas implementasi penegakan hukumnya⁶.

Sementara itu, perkembangan teknologi informasi yang berlangsung sangat cepat telah memunculkan berbagai bentuk kejahatan siber baru yang semakin kompleks dan bersifat transnasional, sehingga menimbulkan tantangan serius bagi aparat penegak hukum dalam proses penyidikan maupun pembuktian digital⁷. Berdasarkan kondisi tersebut, kajian yang secara khusus menganalisis efektivitas penegakan hukum pidana terhadap kejahatan siber serta berbagai kendala implementatif yang dihadapi aparat penegak hukum di Indonesia masih relatif terbatas. Oleh karena itu, penelitian ini dilakukan untuk menganalisis efektivitas penegakan hukum pidana terhadap kejahatan siber serta mengidentifikasi berbagai tantangan dalam implementasinya di era perkembangan teknologi informasi.

Dengan demikian, penelitian mengenai penegakan hukum pidana terhadap kejahatan siber menjadi sangat penting untuk mengidentifikasi berbagai permasalahan yang muncul dalam praktik serta merumuskan solusi yang dapat meningkatkan efektivitas sistem hukum dalam menghadapi kejahatan berbasis teknologi. Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana perkembangan kejahatan siber dalam era teknologi informasi?
2. Bagaimana kerangka hukum pidana dalam penanggulangan kejahatan siber di Indonesia?
3. Apa saja tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan siber?

³ Putra, T. H., & Firdaus, S. U. (2024). Law enforcement against cyber crime in electronic transactions in Indonesia. *International Journal of Multidisciplinary Science*, 3(2), 88–99.

⁴ Imran, M. F. (2023). Preventing and combating cybercrime in Indonesia. *International Journal of Cyber Criminology*, 17(1), 45–60.

⁵ Widijowati, D. (2022). Legal complexity in dealing with cyber crime in Indonesia. *Research Horizon*, 2(4), 423–431.

⁶ Ramadani, S., & Anwar, R. (2024). Validity of electronic documents as legal evidence according to electronic information and transactions law. *Asy-Syar'iyah Journal*, 8(2), 210–222.

⁷ Putra, T. H., & Firdaus, S. U.

Penelitian ini bertujuan untuk menganalisis efektivitas penegakan hukum pidana terhadap kejahatan siber di Indonesia serta mengidentifikasi berbagai kendala yang dihadapi dalam implementasi regulasi yang ada.

2. Metode Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif yang berfokus pada analisis terhadap norma-norma hukum yang mengatur kejahatan siber serta penerapannya dalam sistem hukum di Indonesia. Penelitian hukum normatif dilakukan dengan mengkaji berbagai peraturan perundang-undangan, doktrin hukum, serta literatur akademik yang relevan dengan topik penelitian.

Pendekatan penelitian yang digunakan dalam penelitian ini meliputi beberapa pendekatan, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan digunakan untuk menganalisis berbagai regulasi yang mengatur kejahatan siber di Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik. Pendekatan konseptual digunakan untuk memahami konsep-konsep hukum yang berkaitan dengan *cybercrime* dan penegakan hukum pidana. Sementara itu, pendekatan kasus digunakan untuk menelaah berbagai praktik penegakan hukum terhadap kejahatan siber yang terjadi di Indonesia.

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016. Bahan hukum sekunder meliputi buku, artikel jurnal ilmiah, serta hasil penelitian yang berkaitan dengan hukum siber dan kejahatan siber. Adapun bahan hukum tersier meliputi kamus hukum, ensiklopedia, serta berbagai sumber referensi lain yang mendukung penelitian.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelaah berbagai literatur yang relevan dengan topik penelitian. Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode penalaran hukum secara deduktif, yaitu dengan menarik kesimpulan dari norma-norma hukum yang bersifat umum menuju pada analisis permasalahan yang lebih spesifik terkait penegakan hukum terhadap kejahatan siber.

3. Hasil dan Pembahasan

a. Perkembangan Kejahatan Siber dalam era Teknologi Informasi

1) Karakteristik Kejahatan Siber

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam pola terjadinya tindak pidana. Kejahatan yang sebelumnya dilakukan secara konvensional kini berkembang menjadi kejahatan berbasis teknologi yang dikenal sebagai kejahatan siber (*cybercrime*). *Cybercrime* merupakan bentuk tindak pidana yang dilakukan dengan

memanfaatkan teknologi komputer, jaringan internet, maupun sistem informasi sebagai sarana atau target kejahatan⁸.

Secara konseptual, *cybercrime* memiliki karakteristik yang berbeda dengan kejahatan konvensional. Pertama, *cybercrime* bersifat borderless atau tidak mengenal batas wilayah negara. Pelaku dapat melakukan tindak pidana dari satu negara dan menyerang sistem komputer yang berada di negara lain tanpa harus berada secara fisik di lokasi tersebut⁹. Hal ini menyebabkan penegakan hukum menjadi lebih kompleks karena melibatkan yurisdiksi lintas negara.

Kedua, *cybercrime* memiliki karakter anonimitas tinggi. Teknologi digital memungkinkan pelaku menyembunyikan identitasnya melalui penggunaan *Virtual Private Network (VPN)*, *proxy server*, atau teknik enkripsi lainnya sehingga sulit dilacak oleh aparat penegak hukum¹⁰.

Ketiga, *cybercrime* memiliki sifat dinamis dan cepat berkembang mengikuti perkembangan teknologi informasi. Bentuk-bentuk kejahatan siber terus mengalami perubahan seiring munculnya teknologi baru seperti *cloud computing*, *artificial intelligence*, dan *blockchain*.

Selain itu, *cybercrime* juga memiliki karakteristik kerugian yang luas dan cepat menyebar. Serangan terhadap sistem digital dapat menimbulkan kerugian ekonomi yang besar dalam waktu singkat karena dapat menjangkau korban dalam jumlah besar secara simultan.

Karakteristik lain dari *cybercrime* adalah ketergantungan pada bukti elektronik. Dalam tindak pidana siber, pembuktian tidak lagi bergantung pada bukti fisik konvensional, melainkan pada data digital seperti *log server*, *metadata*, email, atau rekaman transaksi elektronik¹¹. Dengan karakteristik tersebut, *cybercrime* menjadi salah satu bentuk kejahatan modern yang menuntut pendekatan penegakan hukum yang berbeda dengan penanganan kejahatan konvensional.

2) Jenis-Jenis *Cybercrime* yang Berkembang di Masyarakat

Seiring meningkatnya penggunaan teknologi digital, berbagai bentuk *cybercrime* juga semakin berkembang di masyarakat. Salah satu bentuk yang paling umum adalah penipuan online (*online fraud*). Kejahatan ini dilakukan dengan memanfaatkan platform digital seperti marketplace, media sosial, maupun aplikasi pesan instan untuk menipu korban agar mentransfer sejumlah uang¹².

⁸ Imran, M. F. (2023). Preventing and combating cybercrime in Indonesia. *International Journal of Cyber Criminology*, 17(1), 45–60.

⁹ Banjarani, D. R., & Rahmadhani, A. N. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era digital di Indonesia. *Jurnal Yustisia*, 13(2), 145–158.

¹⁰ Nugroho, T., & Soesatyo, B. (2025). Problems of cyber law enforcement against cyber crimes using VPN technology in Indonesia. *Jurnal Greenation Sosial dan Politik*, 4(1), 33–45.

¹¹ Achyarsyah, P., Riyadi, S., & Widodo, K. (2025). The role of digital evidence in criminal law enforcement: Challenges of authentication and admissibility in court. *Research Horizon*, 5(2), 112–124

¹² Syahfallah, Z. A., Razak, A., & Salle, S. (2025). The effectiveness of law enforcement on cybercrime: A case study of online fraud in South Sulawesi. *SiGn Jurnal Hukum*, 7(2), 215–229.

Jenis *cybercrime* lainnya adalah peretasan sistem komputer (*hacking*). Dalam kejahatan ini, pelaku mengakses sistem komputer tanpa izin untuk mencuri data, merusak sistem, atau memperoleh keuntungan tertentu¹³.

Selain itu, terdapat pula pencurian identitas (*identity theft*) yang dilakukan dengan memanfaatkan data pribadi korban seperti nomor kartu kredit, identitas digital, maupun informasi keuangan untuk melakukan transaksi ilegal¹⁴.

Kejahatan lain yang semakin meningkat adalah serangan *malware* dan *ransomware*. Dalam serangan ini, pelaku menyebarkan perangkat lunak berbahaya untuk menginfeksi sistem komputer korban dan kemudian meminta tebusan agar sistem tersebut dapat kembali diakses. Bentuk *cybercrime* lainnya meliputi:

- a) *Carding*, yaitu pencurian data kartu kredit untuk melakukan transaksi ilegal.
- b) *Cyberbullying*, yaitu tindakan intimidasi atau pelecehan melalui media digital.
- c) Penyebaran konten ilegal, seperti pornografi anak atau ujaran kebencian.
- d) *Skimming*, yaitu pencurian data kartu ATM melalui perangkat elektronik tertentu.

Perkembangan jenis *cybercrime* ini menunjukkan bahwa kejahatan siber tidak hanya menimbulkan kerugian ekonomi, tetapi juga berdampak pada keamanan nasional, perlindungan data pribadi, serta stabilitas sistem digital. Di Indonesia, bentuk kejahatan siber yang paling dominan terjadi adalah *phishing*, penyalahgunaan data pribadi, serta penipuan online yang memanfaatkan media digital dan transaksi elektronik. Kejahatan tersebut terus mengalami peningkatan seiring dengan tingginya penggunaan internet, media sosial, dan layanan keuangan digital di masyarakat. Selain menimbulkan kerugian ekonomi, kejahatan tersebut juga berdampak pada keamanan data pribadi dan menurunkan tingkat kepercayaan masyarakat terhadap keamanan sistem digital¹⁵.

3) Faktor Penyebab Meningkatnya Kejahatan Siber

Meningkatnya kasus *cybercrime* tidak terlepas dari beberapa faktor yang mendorong terjadinya kejahatan tersebut. Faktor pertama adalah meningkatnya penetrasi internet dan digitalisasi masyarakat. Semakin banyak masyarakat yang menggunakan internet untuk berbagai aktivitas seperti transaksi keuangan, komunikasi, maupun bisnis digital, sehingga peluang terjadinya kejahatan siber juga semakin besar¹⁶.

Faktor kedua adalah rendahnya literasi digital masyarakat. Banyak pengguna internet yang belum memahami risiko keamanan digital sehingga mudah menjadi korban penipuan online atau serangan *phishing*. Faktor ketiga adalah keterbatasan kemampuan aparat penegak hukum dalam bidang teknologi informasi. Tidak semua aparat penegak

¹³ Widiowati, D. (2022). Legal complexity in dealing with cyber crime in Indonesia. *Research Horizon*, 2(4), 423–431.

¹⁴ Imran, M. F. (2023).

¹⁵ Banjarani, D. R., & Rahmadhani, A. N.

¹⁶ Imran, M. F. (2023) *op cit*

hukum memiliki keahlian dalam digital forensics maupun investigasi siber sehingga proses penanganan *cybercrime* sering mengalami kendala teknis¹⁷.

Faktor keempat adalah perkembangan teknologi yang sangat cepat sehingga regulasi yang ada seringkali tertinggal dibandingkan dengan perkembangan modus operandi kejahatan siber¹⁸. Selain itu, faktor lain yang turut mempengaruhi meningkatnya *cybercrime* adalah keuntungan ekonomi yang besar dengan risiko relatif rendah bagi pelaku. Dibandingkan dengan kejahatan konvensional, *cybercrime* dapat dilakukan dengan biaya operasional yang lebih kecil namun memiliki potensi keuntungan yang besar¹⁹. Dengan berbagai faktor tersebut, *cybercrime* menjadi salah satu bentuk kejahatan yang terus meningkat seiring dengan perkembangan teknologi informasi.

b. Kerangka Hukum Pidana dalam Penanggulangan Kejahatan Siber di Indonesia

1) Analisis Regulasi Terkait Kejahatan Siber

Dalam rangka mengatasi kejahatan siber, Indonesia telah mengembangkan berbagai regulasi hukum yang mengatur aktivitas digital. Regulasi utama yang mengatur *cybercrime* adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016.

UU ITE merupakan landasan hukum yang mengatur berbagai aspek transaksi elektronik, perlindungan data digital, serta penindakan terhadap berbagai bentuk kejahatan siber²⁰. Beberapa pasal penting dalam UU ITE yang berkaitan dengan *cybercrime* antara lain:

- a) Pasal 27: mengatur tentang distribusi konten ilegal
- b) Pasal 28: mengatur tentang penyebaran berita bohong dan ujaran kebencian
- c) Pasal 30: mengatur tentang akses ilegal terhadap sistem elektronik
- d) Pasal 32: mengatur tentang manipulasi data elektronik
- e) Pasal 36: mengatur tentang perbuatan yang menimbulkan kerugian melalui sistem elektronik

Selain UU ITE, penanggulangan *cybercrime* juga diatur dalam beberapa peraturan lain seperti:

- a. Kitab Undang-Undang Hukum Pidana (KUHP)
- b. Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
- c. Undang-Undang Perlindungan Data Pribadi Tahun 2022

¹⁷ Gustryan, M., & Sulaiman, A. (2025). The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating cybercrime through a criminal law approach in Indonesia. *Global International Journal of Law and Social Sciences*, 3(1), 12–23.

¹⁸ Putra, T. H., & Firdaus, S. U. (2024). Law enforcement against cyber crime in electronic transactions in Indonesia. *International Journal of Multidisciplinary Science*, 3(2), 88–99.

¹⁹ Banjarani, D. R., & Rahmadhani, A. N. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era digital di Indonesia. *Jurnal Yustisia*, 13(2), 145–158.

²⁰ Lubis, M., & Maulana, F. A. (2010). Information and electronic transaction law effectiveness (UU-ITE) in Indonesia. *Proceedings of the International Conference on Computer Engineering and Applications*.

Meskipun UU ITE menjadi landasan utama dalam penanggulangan kejahatan siber di Indonesia, dalam praktiknya regulasi tersebut masih menuai berbagai kritik. Beberapa ketentuan dalam UU ITE dinilai memiliki rumusan norma yang multitafsir sehingga berpotensi menimbulkan ketidakpastian hukum dalam penerapannya. Salah satu pasal yang sering menjadi perdebatan adalah ketentuan mengenai penghinaan dan pencemaran nama baik melalui media elektronik yang dianggap memiliki interpretasi yang luas dan berpotensi membatasi kebebasan berekspresi di ruang digital²¹. Selain itu, beberapa kalangan juga menilai bahwa penerapan UU ITE cenderung mengarah pada overcriminalization karena terdapat perluasan kriminalisasi terhadap tindakan tertentu di ruang siber yang seharusnya dapat diselesaikan melalui mekanisme nonpidana.

Di sisi lain, regulasi penanggulangan kejahatan siber di Indonesia juga perlu dibandingkan dengan instrumen hukum internasional seperti *Convention on Cybercrime* atau *Budapest Convention* yang disusun oleh *Council of Europe* pada tahun 2001. Budapest Convention merupakan instrumen internasional pertama yang secara khusus mengatur penanganan cybercrime melalui harmonisasi hukum pidana, prosedur investigasi digital, serta penguatan kerja sama internasional dalam penanggulangan kejahatan siber lintas negara²². Dibandingkan dengan *Budapest Convention*, pengaturan *cybercrime* di Indonesia masih menghadapi tantangan dalam aspek kerja sama internasional, mekanisme pertukaran bukti elektronik lintas negara, serta standardisasi prosedur investigasi digital. Oleh karena itu, penguatan regulasi nasional perlu dilakukan agar selaras dengan perkembangan hukum internasional dan dinamika kejahatan siber global. Regulasi tersebut menunjukkan bahwa pemerintah Indonesia telah berupaya membangun kerangka hukum yang komprehensif untuk menangani kejahatan siber.

2) Peran Hukum Pidana dalam Mengatur Aktivitas Digital

Hukum pidana memiliki posisi yang sangat penting dalam mengatur aktivitas digital dan menanggulangi kejahatan siber di tengah perkembangan teknologi informasi yang semakin pesat. Dalam perspektif kebijakan hukum pidana (*criminal law policy*), penggunaan hukum pidana terhadap cybercrime merupakan bagian dari kebijakan negara dalam melindungi masyarakat dari berbagai bentuk penyalahgunaan teknologi informasi. Kebijakan hukum pidana tidak hanya diarahkan pada pemberian sanksi terhadap pelaku kejahatan, tetapi juga bertujuan menciptakan ketertiban, keamanan, dan perlindungan hukum bagi masyarakat di ruang digital²³.

Dalam konteks aktivitas digital, hukum pidana berfungsi sebagai instrumen pengendalian sosial (*social control*) untuk mengatur perilaku masyarakat agar penggunaan teknologi informasi tetap berada dalam batas-batas yang sesuai dengan norma hukum.

²¹ Widijowati, D. (2022). Legal complexity in dealing with cyber crime in Indonesia. *Research Horizon*, 2(4), 423–431.

²² Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

²³ Arief, B. N. (2016). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru. Kencana.

Melalui ketentuan pidana yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), negara memiliki kewenangan untuk menindak berbagai bentuk penyalahgunaan sistem elektronik seperti akses ilegal, pencurian data pribadi, penipuan online, manipulasi informasi elektronik, hingga penyebaran konten yang melanggar hukum²⁴. Dengan demikian, keberadaan hukum pidana di ruang siber menjadi penting untuk menjaga keamanan dan stabilitas sistem digital di tengah meningkatnya ketergantungan masyarakat terhadap teknologi informasi.

Selain memiliki fungsi represif melalui pemberian sanksi pidana, hukum pidana juga memiliki fungsi preventif dalam mencegah terjadinya *cybercrime*. Keberadaan aturan pidana diharapkan dapat memberikan efek pencegahan (*deterrent effect*) bagi masyarakat agar tidak melakukan penyalahgunaan teknologi informasi. Dalam teori kebijakan hukum pidana, penggunaan sarana penal harus ditempatkan sebagai bagian dari kebijakan sosial yang lebih luas untuk melindungi masyarakat (*social defence*) dan mewujudkan kesejahteraan sosial (*social welfare*)²⁵. Oleh karena itu, penanggulangan *cybercrime* tidak cukup hanya dilakukan melalui pemidanaan, tetapi juga perlu didukung dengan penguatan literasi digital, peningkatan keamanan sistem elektronik, serta pengembangan regulasi yang adaptif terhadap perkembangan teknologi.

Meskipun demikian, penerapan hukum pidana dalam mengatur aktivitas digital juga perlu dilakukan secara proporsional agar tidak menimbulkan *overcriminalization* maupun pembatasan terhadap kebebasan berekspresi di ruang digital. Oleh sebab itu, kebijakan hukum pidana terhadap *cybercrime* harus mampu menciptakan keseimbangan antara perlindungan kepentingan masyarakat, kepastian hukum, dan penghormatan terhadap hak asasi manusia di era digital.

3) Kewenangan Aparat Penegak Hukum dalam Penindakan *Cybercrime*

Penegakan hukum terhadap *cybercrime* di Indonesia melibatkan berbagai lembaga penegak hukum, seperti Kepolisian, Kejaksaan, dan Pengadilan. Kepolisian Republik Indonesia memiliki unit khusus yang menangani kejahatan siber, yaitu Direktorat Tindak Pidana Siber Bareskrim Polri, yang bertugas melakukan penyelidikan dan penyidikan terhadap berbagai tindak pidana berbasis teknologi informasi²⁶. Selain itu, dalam proses pembuktian perkara *cybercrime*, aparat penegak hukum juga bekerja sama dengan ahli digital forensik untuk menganalisis bukti elektronik seperti perangkat komputer, telepon seluler, maupun data transaksi digital²⁷. Selanjutnya, kejaksaan memiliki kewenangan dalam proses penuntutan, sedangkan pengadilan berperan dalam memeriksa dan memutus perkara berdasarkan alat bukti elektronik yang diajukan.

²⁴ Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.

²⁵ Arief, B. N. (2016). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru. Kencana

²⁶ Putra, T. H., & Firdaus, S. U. (2024). Law enforcement against cyber crime in electronic transactions in Indonesia. *International Journal of Multidisciplinary Science*, 3(2), 88–99.

²⁷ Zulkifli, Z., Marlina, M., & Akhyar, A. (2021). Role and status of digital forensic experts in analyzing digital evidence on cybercrime cases. *Jurnal Ilmiah Metadata*, 3(1), 45–56.

Meskipun pembagian kewenangan antar lembaga penegak hukum telah diatur, dalam praktiknya efektivitas kelembagaan dalam penanganan *cybercrime* masih menghadapi berbagai hambatan struktural dan teknis. Salah satu kendala utama adalah keterbatasan sumber daya manusia yang memiliki kompetensi khusus di bidang teknologi informasi dan digital forensik. Tidak seluruh aparat penegak hukum memiliki kemampuan yang memadai dalam melakukan investigasi siber maupun analisis bukti elektronik, sehingga proses penanganan perkara seringkali membutuhkan waktu yang lebih lama dibandingkan tindak pidana konvensional²⁸.

Selain itu, koordinasi antar lembaga penegak hukum dalam penanganan *cybercrime* juga belum berjalan secara optimal. Dalam beberapa kasus, masih ditemukan hambatan dalam pertukaran data, sinkronisasi proses penyidikan dan penuntutan, serta keterbatasan akses terhadap data digital yang berada di luar yurisdiksi Indonesia. Kondisi tersebut menunjukkan bahwa penegakan hukum terhadap kejahatan siber tidak hanya memerlukan regulasi yang memadai, tetapi juga membutuhkan penguatan kelembagaan dan koordinasi antar lembaga secara berkelanjutan.

Dalam praktiknya, berbagai kasus kebocoran data pribadi dan penipuan online di Indonesia menunjukkan bahwa kejahatan siber berkembang lebih cepat dibandingkan kapasitas penegakan hukumnya. Salah satu contoh adalah maraknya kasus kebocoran data digital dan penyalahgunaan identitas elektronik yang sulit ditangani secara optimal karena keterbatasan kemampuan pelacakan digital dan karakter kejahatan yang bersifat lintas negara. Hal tersebut memperlihatkan bahwa tantangan utama dalam penegakan hukum *cybercrime* tidak hanya terletak pada aspek regulasi, tetapi juga pada kesiapan kelembagaan dalam menghadapi perkembangan teknologi digital yang semakin kompleks.

Oleh karena itu, diperlukan penguatan kapasitas kelembagaan melalui peningkatan kompetensi aparat penegak hukum, pengembangan infrastruktur digital forensik, serta penguatan kerja sama antar lembaga dan kerja sama internasional agar proses penegakan hukum terhadap *cybercrime* dapat berjalan lebih efektif dan adaptif terhadap perkembangan teknologi informasi.

c. Tantangan Penegakan Hukum terhadap Kejahatan Siber

1) Kendala Teknis, Yuridis dan Kelembagaan

Meskipun Indonesia telah memiliki berbagai regulasi yang mengatur *cybercrime*, dalam praktiknya penegakan hukum terhadap kejahatan siber masih menghadapi berbagai kendala. Salah satu kendala utama adalah keterbatasan infrastruktur teknologi dan sumber daya manusia dalam bidang *digital forensics*²⁹. Investigasi *cybercrime* memerlukan peralatan teknologi canggih serta tenaga ahli yang memiliki kemampuan khusus dalam analisis data digital.

²⁸ Gustryan, M., & Sulaiman, A. (2025). The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating cybercrime through a criminal law approach in Indonesia. *Global International Journal of Law and Social Sciences*, 3(1), 12–23.

²⁹ Ibid

Selain itu, terdapat pula kendala koordinasi antar lembaga penegak hukum yang seringkali belum berjalan secara optimal sehingga proses penanganan kasus menjadi lambat³⁰. Dari sisi yuridis, beberapa ketentuan dalam UU ITE masih menimbulkan perdebatan terkait interpretasi hukum, terutama mengenai batasan perbuatan yang dapat dikategorikan sebagai tindak pidana siber.

2) Masalah Pembuktian dalam Tindak Pidana Siber

Salah satu tantangan terbesar dalam penegakan hukum *cybercrime* adalah pembuktian di pengadilan. Dalam tindak pidana siber, alat bukti utama berupa bukti elektronik yang memiliki karakteristik berbeda dengan bukti konvensional. Bukti elektronik bersifat mudah berubah, mudah dipindahkan, dan mudah dihapus sehingga memerlukan prosedur khusus dalam pengumpulan dan penyimpanannya³¹. Selain itu, proses autentikasi dan verifikasi bukti digital juga memerlukan keahlian teknis yang tinggi agar dapat diterima sebagai alat bukti yang sah di pengadilan³².

3) Karakter Lintas Negara (*Transnational Crime*)

Cybercrime seringkali memiliki karakter transnasional, dimana pelaku, korban, dan server yang digunakan berada di negara yang berbeda. Kondisi ini menyebabkan penegakan hukum menjadi lebih kompleks karena memerlukan kerja sama internasional dalam proses penyelidikan dan penuntutan. Selain itu, perbedaan sistem hukum antar negara juga dapat menjadi hambatan dalam proses ekstradisi maupun pertukaran data digital.

d. Optimalisasi Penegakan Hukum Pidana terhadap Kejahatan Siber

1) Penguatan Regulasi

Upaya optimalisasi penegakan hukum terhadap *cybercrime* perlu dilakukan melalui penguatan regulasi yang adaptif terhadap perkembangan teknologi digital. Reformasi regulasi diperlukan untuk menyesuaikan ketentuan hukum dengan perkembangan modus operandi kejahatan siber yang semakin kompleks.

2) Peningkatan Kapasitas Aparat Penegak Hukum

Peningkatan kapasitas aparat penegak hukum merupakan faktor penting dalam meningkatkan efektivitas penegakan hukum terhadap *cybercrime*. Hal ini dapat dilakukan melalui:

- a) Pelatihan digital forensics;
- b) Peningkatan kemampuan investigasi siber;
- c) Penguatan unit *cybercrime* di lembaga penegak hukum³³.

³⁰ Nugroho, T., & Soesatyo, B. (2025). Problems of cyber law enforcement against cyber crimes using VPN technology in Indonesia. *Jurnal Greenation Sosial dan Politik*, 4(1), 33–45.

³¹ Achyarsyah, P., Riyadi, S., & Widodo, K. (2025). The role of digital evidence in criminal law enforcement: Challenges of authentication and admissibility in court. *Research Horizon*, 5(2), 112–124.

³² Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest: Journal of Universal Studies*, 4(3), 1560–1572.

³³ Gustryan, M., & Sulaiman, A. (2025). The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating *cybercrime* through a criminal law approach in Indonesia. *Global International Journal of Law and Social Sciences*, 3(1), 12–23.

3) Kerja Sama Internasional

Karakter cybercrime yang bersifat lintas negara menuntut adanya kerja sama internasional dalam penanggulangan kejahatan tersebut. Kerja sama ini dapat dilakukan melalui:

- a) Perjanjian ekstradisi;
- b) Pertukaran informasi intelijen;
- c) Kerja sama investigasi lintas negara³⁴.

4) Pendekatan Preventif dan Represif

Penanggulangan cybercrime tidak hanya mengandalkan pendekatan represif melalui penegakan hukum pidana, tetapi juga memerlukan pendekatan preventif. Pendekatan preventif dapat dilakukan melalui:

- a) Peningkatan literasi digital masyarakat;
- b) Penguatan sistem keamanan siber;
- c) Edukasi penggunaan internet yang aman³⁵.

Dengan kombinasi pendekatan preventif dan represif, diharapkan upaya penanggulangan cybercrime dapat dilakukan secara lebih efektif dan berkelanjutan.

4. Penutup

Perkembangan teknologi informasi telah mendorong munculnya berbagai bentuk kejahatan siber (cybercrime) yang memiliki karakteristik berbeda dengan kejahatan konvensional, seperti bersifat lintas batas negara, memiliki tingkat anonimitas tinggi, serta bergantung pada bukti elektronik dalam proses pembuktiannya. Bentuk cybercrime yang berkembang di masyarakat antara lain penipuan online, peretasan sistem komputer, pencurian identitas, penyebaran malware, carding, hingga skimming.

Indonesia telah memiliki kerangka hukum dalam penanggulangan kejahatan siber melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 serta didukung oleh peraturan lain seperti KUHP, KUHPA, dan Undang-Undang Perlindungan Data Pribadi. Regulasi tersebut memberikan dasar hukum bagi aparat penegak hukum dalam menindak berbagai bentuk kejahatan yang terjadi di ruang siber.

Namun demikian, efektivitas penegakan hukum terhadap cybercrime masih menghadapi berbagai tantangan, seperti keterbatasan sumber daya manusia yang memiliki keahlian di bidang teknologi informasi, kendala teknis dalam proses pembuktian digital, serta karakter kejahatan siber yang bersifat lintas negara. Oleh karena itu, penegakan hukum pidana terhadap cybercrime memerlukan pendekatan yang lebih adaptif dan komprehensif agar mampu mengikuti perkembangan teknologi informasi yang semakin pesat.

³⁴ Banjarani, D. R., & Rahmadhani, A. N. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era digital di Indonesia. *Jurnal Yustisia*, 13(2), 145–158.

³⁵ Imran, M. F. (2023). Preventing and combating cybercrime in Indonesia. *International Journal of Cyber Criminology*, 17(1), 45–60.

5. Daftar Pustaka

- Achyarsyah, P., Riyadi, S., & Widodo, K. (2025). The role of digital evidence in criminal law enforcement: Challenges of authentication and admissibility in court. *Research Horizon*, 5(2), 112–124.
<https://journal.lifescifi.com/index.php/RH/article/view/950>
- Arief, B. N. (2016). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru. Kencana.
- Auliaurrahman, A., & Anshari, N. (2025). The existence and regulation of cyber law: The government's role in combating digital crime in Indonesia. *Jurisprudensi: Jurnal Ilmu Syariah dan Hukum*, 12(1), 45–58.
<https://dev-journal.iainlangsa.ac.id/index.php/jurisprudensi/article/view/10612>
- Banjarani, D. R., & Rahmadhani, A. N. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era digital di Indonesia. *Jurnal Yustisia*, 13(2), 145–158.
<https://jurnal.untirta.ac.id/index.php/yustisia/article/download/29046/15484>
- Brenner, S. W. (2010). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.
<https://doi.org/10.2307/j.ctv1rcf0t>
- Brenner, S. W. (2012). *Cybercrime: Criminal threats from cyberspace*. Praeger.
<https://doi.org/10.5040/9780313392422>
- Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Academic Press.
<https://doi.org/10.1016/C2009-0-61100-0>
- Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.
<https://doi.org/10.1017/CBO9781139540844>
- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest: Journal of Universal Studies*, 4(3), 1560–1572.
<http://eduvest.greenvest.co.id/index.php/edv/article/view/1812>
- Grabosky, P. (2016). *Cybercrime*. Routledge.
<https://doi.org/10.4324/9781315720930>
- Gustryan, M., & Sulaiman, A. (2025). The urgency of regulatory reformulation and strengthening the capacity of law enforcers in combating cybercrime through a criminal law approach in Indonesia. *Global International Journal of Law and Social Sciences*, 3(1), 12–23.
<https://research.e-greenation.org/GIJLSS/article/view/416>
- Imran, M. F. (2023). Preventing and combating cybercrime in Indonesia. *International Journal of Cyber Criminology*, 17(1), 45–60.
<https://www.cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/225>

- Interpol. (2023). Global cybercrime report.
<https://www.interpol.int/en/Crimes/Cybercrime>
- Kshetri, N. (2021). Cybercrime and cyber-security issues in developing economies. Springer.
<https://doi.org/10.1007/978-3-030-68453-3>
- Lubis, M., & Maulana, F. A. (2010). Information and electronic transaction law effectiveness (UU-ITE) in Indonesia. Proceedings of the International Conference on Computer Engineering and Applications.
<https://ieeexplore.ieee.org/document/5971892>
- Martono, M., & Akbar, M. G. G. (2025). Law enforcement of transnational cybercrime: Case study in Indonesia. *De Lega Lata: Jurnal Ilmu Hukum*, 10(2), 140–154.
<https://jurnal.umsu.ac.id/index.php/delegalata/article/view/24627>
- Nugroho, T., & Soesatyo, B. (2025). Problems of cyber law enforcement against cyber crimes using VPN technology in Indonesia. *Jurnal Greenation Sosial dan Politik*, 4(1), 33–45.
<https://greenationpublisher.org/JGSP/article/view/492>
- Putra, T. H., & Firdaus, S. U. (2024). Law enforcement against cyber crime in electronic transactions in Indonesia. *International Journal of Multidisciplinary Science*, 3(2), 88–99.
<https://www.multisciencejournal.com/index.php/ijm/article/view/430>
- Ramadani, S., & Anwar, R. (2024). Validity of electronic documents as legal evidence according to electronic information and transactions law. *Asy-Syar'iyah Journal*, 8(2), 210–222.
<https://rumahjurnal.iainsasbabel.ac.id/asy/article/view/6399>
- Sari, R. M. P. (2025). Criminal responsibility in cybercrime: An analysis of phishing crimes in Indonesia. *Jurnal Hukum dan Keadilan*, 9(1), 77–90.
<https://jurnalhafasy.com/index.php/jhk/article/view/418>
- Siregar, W., Siregar, A. A., & Siahaan, N. (2026). The position of electronic evidence in the police investigation process based on the criminal procedure code and ITE law. *International Journal of Science and Engineering*, 6(1), 15–27.
<https://ijsenet.com/index.php/IJSE/article/view/376>
- Sunariyo, S., & Elviandri, E. (2025). Sosialisasi pembuktian cyber crime dalam KUHAP dan UU ITE. *Jurnal Sosial Madani Indonesia*, 5(1), 32–44.
<https://syadani.onlinelibrary.id/index.php/JS/article/view/403>
- Syahfallah, Z. A., Razak, A., & Salle, S. (2025). The effectiveness of law enforcement on cybercrime: A case study of online fraud in South Sulawesi. *SIGn Jurnal Hukum*, 7(2), 215–229.
<https://www.jurnal.penerbitsign.com/index.php/sjh/article/view/v7n2-29>
- United Nations Office on Drugs and Crime. (2022). Comprehensive study on cybercrime.
<https://www.unodc.org/unodc/en/cybercrime/global-study-on-cybercrime.html>
- Wall, D. S. (2017). Cybercrime: The transformation of crime in the information age. Polity Press.
<https://politybooks.com/bookdetail/?isbn=9780745652958>

- Wiarti, J. (2023). Legality of electronic evidence in cyber crime cases. Ahmad Dahlan Indonesian Law Journal, 8(1), 1-10.
- Widijowati, D. (2022). Legal complexity in dealing with cyber crime in Indonesia. Research Horizon, 2(4), 423-431.
<http://journal.lifescifi.com/index.php/RH/article/view/98>
- World Economic Forum. (2023). Global cybersecurity outlook.
<https://www.weforum.org/reports/global-cybersecurity-outlook-2023>
- Zulkifli, Z., Marlina, M., & Akhyar, A. (2021). Role and status of digital forensic experts in analyzing digital evidence on cybercrime cases. Jurnal Ilmiah Metadata, 3(1), 45-56.
<https://ejournal.steitholabulilmi.ac.id/index.php/metadata/article/view/51>