

Hukum Pidana dan Perkembangan Teknologi Informasi di Indonesia

Angga Praditya Alif Handriawan

Universitas Widya Mataram, Yogyakarta, Indonesia

E-mail: anggapraditya425@gmail.com

Article History:

Received: 06 Juli 2026

Revised: 18 Juli 2026

Accepted: 01 Agustus 2026

Keywords: Hukum Pidana, Teknologi Informasi, Kejahatan Siber, UU ITE.

Abstrak: Perkembangan teknologi informasi (TI) telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam bidang hukum pidana. Kemajuan digital menghadirkan bentuk-bentuk kejahatan baru yang tidak sepenuhnya dapat dijangkau oleh hukum pidana konvensional. Artikel ini bertujuan untuk menganalisis bagaimana hukum pidana beradaptasi terhadap perkembangan teknologi informasi serta mengkaji efektivitas regulasi yang ada dalam menangani kejahatan siber di Indonesia. Metode yang digunakan adalah pendekatan yuridis normatif dengan menelaah peraturan perundang-undangan dan literatur ilmiah terbaru. Hasil kajian menunjukkan bahwa meskipun Indonesia telah memiliki regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), masih terdapat tantangan dalam implementasi, penegakan hukum, serta penyesuaian terhadap dinamika teknologi yang terus berkembang.

PENDAHULUAN

Perkembangan teknologi informasi dalam beberapa dekade terakhir telah membawa perubahan yang sangat signifikan dalam kehidupan manusia. Transformasi digital tidak hanya memengaruhi cara manusia berkomunikasi, tetapi juga mengubah pola kerja, sistem ekonomi, hingga interaksi sosial secara keseluruhan. Kehadiran internet, perangkat pintar, serta berbagai platform digital telah menciptakan ruang baru yang memungkinkan aktivitas dilakukan secara lebih cepat, efisien, dan tanpa batas geografis. Dalam konteks ini, teknologi informasi menjadi tulang punggung utama dalam era globalisasi dan digitalisasi yang semakin berkembang pesat. Kemajuan teknologi informasi juga mendorong lahirnya berbagai inovasi di bidang ekonomi, seperti *e-commerce*, *financial technology (fintech)*, dan ekonomi berbasis platform. Aktivitas perdagangan yang sebelumnya dilakukan secara konvensional kini beralih ke sistem digital yang memungkinkan transaksi dilakukan kapan saja dan di mana saja. Hal ini memberikan kemudahan bagi masyarakat sekaligus meningkatkan pertumbuhan ekonomi secara signifikan. Namun, kemudahan tersebut juga membuka peluang bagi pihak-pihak tertentu untuk melakukan penyalahgunaan teknologi dalam bentuk tindakan kriminal. Di balik berbagai manfaat yang ditawarkan, perkembangan teknologi informasi juga menimbulkan dampak negatif, khususnya dalam bentuk kejahatan siber (*cybercrime*). Kejahatan ini meliputi berbagai tindakan seperti penipuan *online*, peretasan (*hacking*), pencurian identitas, penyalahgunaan data pribadi, hingga penyebaran informasi palsu (*hoaks*) dan ujaran kebencian. Kejahatan siber memiliki karakteristik yang berbeda dengan

kejahatan konvensional karena dilakukan melalui jaringan digital yang sulit dilacak serta sering melibatkan pelaku lintas negara (Agustian, 2021).

Sifat kejahatan siber yang anonim dan *borderless* menjadi tantangan tersendiri bagi sistem hukum pidana. Pelaku kejahatan dapat dengan mudah menyembunyikan identitasnya menggunakan teknologi tertentu, seperti *virtual private network* (VPN) atau akun palsu. Selain itu, lokasi pelaku dan korban yang berada di negara berbeda menyulitkan proses penegakan hukum karena melibatkan yurisdiksi lintas negara. Hal ini menunjukkan bahwa hukum pidana konvensional memiliki keterbatasan dalam menjangkau perkembangan kejahatan berbasis teknologi informasi. Hukum pidana sebagai instrumen utama dalam menjaga ketertiban dan keamanan masyarakat dituntut untuk mampu beradaptasi dengan perkembangan zaman. Prinsip dasar hukum pidana yang bersifat represif perlu dilengkapi dengan pendekatan yang lebih modern dan responsif terhadap perubahan teknologi. Dalam konteks ini, hukum pidana tidak hanya berfungsi sebagai alat penegakan hukum, tetapi juga sebagai sarana perlindungan terhadap masyarakat dari ancaman kejahatan digital yang semakin kompleks. Sebagai respons terhadap perkembangan teknologi informasi, Indonesia telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016. Regulasi ini menjadi landasan hukum utama dalam mengatur aktivitas digital serta menindak berbagai bentuk kejahatan siber. UU ITE mengatur berbagai aspek, mulai dari transaksi elektronik, perlindungan data, hingga ketentuan pidana bagi pelaku kejahatan di dunia maya. Meskipun demikian, keberadaan UU ITE tidak lepas dari berbagai kritik dan perdebatan. Beberapa pasal dalam undang-undang tersebut dinilai memiliki multitafsir, terutama yang berkaitan dengan pencemaran nama baik dan ujaran kebencian. Hal ini berpotensi menimbulkan penyalahgunaan dalam penegakan hukum, di mana pasal-pasal tersebut digunakan untuk membungkam kebebasan berekspresi. Oleh karena itu, diperlukan evaluasi yang berkelanjutan terhadap regulasi ini agar tetap relevan dan tidak menimbulkan ketidakadilan (Agustian, 2021).

Selain persoalan regulasi, tantangan juga muncul dalam aspek penegakan hukum. Aparat penegak hukum dituntut untuk memiliki kemampuan teknis yang memadai dalam menangani kejahatan siber, termasuk dalam hal *digital forensic* dan analisis data elektronik. Keterbatasan sumber daya manusia serta infrastruktur teknologi menjadi hambatan dalam proses penyidikan dan pembuktian kasus kejahatan digital. Hal ini menunjukkan bahwa adaptasi hukum pidana tidak hanya terbatas pada regulasi, tetapi juga pada peningkatan kapasitas institusi penegak hukum. Di sisi lain, rendahnya tingkat literasi digital masyarakat turut memperburuk kondisi tersebut. Banyak pengguna internet yang belum memahami risiko penggunaan teknologi informasi sehingga rentan menjadi korban kejahatan siber. Kurangnya kesadaran akan pentingnya keamanan data pribadi juga menjadi faktor yang memperbesar potensi terjadinya pelanggaran hukum di dunia digital. Oleh karena itu, upaya pencegahan melalui edukasi masyarakat menjadi bagian penting dalam sistem perlindungan hukum. Berdasarkan uraian tersebut, dapat disimpulkan bahwa perkembangan teknologi informasi membawa dampak yang kompleks terhadap sistem hukum pidana di Indonesia. Di satu sisi, teknologi memberikan kemudahan dan peluang besar dalam berbagai aspek kehidupan, namun di sisi lain juga memunculkan tantangan baru dalam bentuk kejahatan siber. Oleh karena itu, diperlukan upaya yang komprehensif, baik dari segi regulasi, penegakan hukum, maupun kesadaran masyarakat agar hukum pidana dapat berfungsi secara efektif dalam menghadapi dinamika perkembangan teknologi informasi yang terus berubah (Anggreini, 2025).

LANDASAN TEORI

1. Hukum Pidana

Hukum pidana merupakan cabang hukum yang memiliki peran penting dalam menjaga ketertiban dan keamanan masyarakat. Secara umum, hukum pidana mengatur tentang perbuatan-perbuatan yang dilarang oleh negara serta menetapkan sanksi bagi pelanggarnya. Norma dalam hukum pidana bersifat memaksa dan mengikat seluruh warga negara, sehingga pelanggaran terhadap norma tersebut akan dikenai konsekuensi berupa pidana. Dalam konteks ini, hukum pidana berfungsi sebagai alat kontrol sosial untuk mencegah terjadinya tindakan yang merugikan masyarakat. Tujuan utama hukum pidana adalah melindungi kepentingan hukum (*rechtsbelangen*) yang meliputi individu, masyarakat, dan negara. Perlindungan ini diwujudkan melalui pemberian sanksi yang bertujuan memberikan efek jera kepada pelaku serta mencegah orang lain melakukan perbuatan serupa. Selain itu, hukum pidana juga memiliki fungsi edukatif, yaitu memberikan pemahaman kepada masyarakat mengenai batasan-batasan perilaku yang diperbolehkan dan yang dilarang dalam kehidupan sosial (**Anggreini, 2025**).

Dalam perkembangannya, hukum pidana tidak hanya bersifat represif, tetapi juga preventif dan rehabilitatif. Pendekatan represif menitikberatkan pada pemberian hukuman setelah terjadinya tindak pidana, sedangkan pendekatan preventif bertujuan mencegah terjadinya kejahatan melalui berbagai kebijakan dan regulasi. Sementara itu, pendekatan rehabilitatif berfokus pada perbaikan pelaku agar dapat kembali menjadi anggota masyarakat yang produktif. Ketiga pendekatan ini menunjukkan bahwa hukum pidana memiliki dimensi yang kompleks dalam sistem hukum modern (**Anggreini, 2025**).

Hukum pidana di Indonesia sebagian besar masih berlandaskan pada Kitab Undang-Undang Hukum Pidana (KUHP) yang berasal dari warisan kolonial Belanda. Meskipun telah mengalami berbagai perubahan dan pembaruan, KUHP masih menghadapi tantangan dalam menyesuaikan diri dengan perkembangan zaman, khususnya dalam menghadapi kejahatan berbasis teknologi. Oleh karena itu, diperlukan pembaruan hukum pidana yang lebih responsif terhadap dinamika sosial dan perkembangan teknologi informasi. Dalam konteks globalisasi dan digitalisasi, hukum pidana dituntut untuk mampu menjangkau bentuk-bentuk kejahatan baru yang tidak diatur secara eksplisit dalam hukum konvensional. Kejahatan digital seperti pencurian data, penipuan *online*, dan peretasan memerlukan pendekatan hukum yang berbeda karena memiliki karakteristik khusus, seperti tidak mengenal batas wilayah dan menggunakan teknologi canggih. Hal ini menuntut adanya harmonisasi antara hukum nasional dan hukum internasional (**Damayanti, 2026**).

Dengan demikian, hukum pidana harus terus berkembang agar tetap relevan dengan kondisi masyarakat yang dinamis. Pembaruan hukum tidak hanya mencakup aspek substansi, tetapi juga struktur dan kultur hukum. Artinya, selain memperbaiki regulasi, perlu juga meningkatkan kualitas aparat penegak hukum serta kesadaran masyarakat terhadap hukum. Tanpa adanya sinergi antara ketiga aspek tersebut, hukum pidana akan sulit berfungsi secara optimal dalam menjaga ketertiban di era digital (**Damayanti, 2026**).

2. Teknologi Informasi

Teknologi informasi merupakan salah satu faktor utama yang mendorong perubahan dalam berbagai aspek kehidupan modern. Secara umum, teknologi informasi mencakup segala bentuk teknologi yang digunakan untuk mengolah, menyimpan, dan menyebarkan informasi dalam bentuk digital. Perkembangan teknologi ini telah mengubah cara manusia

berkomunikasi, bekerja, belajar, dan berinteraksi secara sosial. Dengan adanya teknologi informasi, akses terhadap informasi menjadi lebih cepat, mudah, dan luas. Salah satu perkembangan paling signifikan dalam teknologi informasi adalah munculnya internet yang menghubungkan berbagai perangkat di seluruh dunia. Internet memungkinkan pertukaran informasi secara real-time tanpa batas geografis, sehingga menciptakan dunia yang semakin terintegrasi. Selain itu, perkembangan media sosial juga telah mengubah pola komunikasi masyarakat menjadi lebih terbuka dan interaktif, meskipun di sisi lain juga menimbulkan berbagai risiko baru (Damayanti, 2026).

Selain internet, teknologi seperti big data, kecerdasan buatan (artificial intelligence), dan blockchain juga turut mempercepat transformasi digital. Big data memungkinkan pengolahan data dalam jumlah besar untuk menghasilkan informasi yang lebih akurat dan relevan. Kecerdasan buatan digunakan untuk meningkatkan efisiensi dalam berbagai sektor, seperti kesehatan, pendidikan, dan industri. Sementara itu, blockchain menawarkan sistem keamanan data yang lebih transparan dan sulit untuk dimanipulasi (Damayanti, 2026).

Perkembangan teknologi informasi memberikan dampak positif yang sangat besar, terutama dalam meningkatkan efisiensi dan produktivitas. Dalam bidang ekonomi, teknologi ini mendorong pertumbuhan e-commerce dan digitalisasi layanan keuangan. Dalam bidang pendidikan, teknologi memungkinkan pembelajaran jarak jauh yang fleksibel. Namun, di balik manfaat tersebut, terdapat pula risiko yang harus diantisipasi, seperti kebocoran data, penyalahgunaan informasi, dan kejahatan siber. Teknologi informasi juga memiliki karakteristik yang dinamis dan terus berkembang. Inovasi teknologi muncul dengan sangat cepat sehingga sering kali regulasi yang ada tidak mampu mengimbangi perkembangan tersebut. Hal ini menimbulkan kesenjangan antara kemajuan teknologi dan kemampuan hukum dalam mengaturnya. Oleh karena itu, diperlukan pendekatan yang adaptif dalam mengelola perkembangan teknologi informasi agar tetap memberikan manfaat bagi masyarakat (Damayanti, 2026).

Dengan demikian, teknologi informasi tidak hanya menjadi alat bantu dalam kehidupan manusia, tetapi juga menjadi faktor yang memengaruhi struktur sosial dan sistem hukum. Perkembangan teknologi harus diimbangi dengan kebijakan yang tepat agar dapat meminimalkan dampak negatif yang ditimbulkan. Peran pemerintah, sektor swasta, dan masyarakat sangat penting dalam menciptakan ekosistem digital yang aman dan berkelanjutan (Damayanti, 2026).

3. Kejahatan Siber (Cybercrime)

Kejahatan siber atau cybercrime merupakan bentuk kejahatan yang memanfaatkan teknologi informasi sebagai sarana utama dalam melakukan tindak pidana. Kejahatan ini dilakukan melalui komputer, jaringan internet, atau perangkat digital lainnya. Berbeda dengan kejahatan konvensional, cybercrime memiliki karakteristik khusus, seperti bersifat anonim, lintas batas negara, dan sulit dilacak. Hal ini menjadikan kejahatan siber sebagai salah satu tantangan terbesar dalam penegakan hukum modern (Fariq et al., 2026).

Salah satu bentuk kejahatan siber yang sering terjadi adalah phishing, yaitu upaya untuk memperoleh informasi sensitif seperti username, password, dan data keuangan dengan cara menipu korban melalui email atau situs palsu. Selain itu, hacking juga menjadi ancaman serius, di mana pelaku memperoleh akses ilegal ke sistem komputer untuk mencuri atau merusak data. Kedua jenis kejahatan ini sering kali menimbulkan kerugian besar, baik bagi individu maupun perusahaan. Carding merupakan bentuk lain dari

kejahatan siber yang melibatkan penggunaan data kartu kredit secara ilegal untuk melakukan transaksi. Kejahatan ini biasanya dilakukan dengan mencuri data kartu kredit melalui berbagai metode, seperti skimming atau peretasan sistem. Selain itu, cyberbullying juga menjadi masalah yang semakin meningkat, terutama di kalangan pengguna media sosial, di mana korban mengalami tekanan psikologis akibat intimidasi atau pelecehan secara online (Fariq et al., 2026).

Penyebaran konten ilegal, seperti pornografi, hoaks, dan ujaran kebencian, juga termasuk dalam kategori kejahatan siber. Konten-konten tersebut dapat dengan mudah menyebar luas melalui internet dan berpotensi menimbulkan dampak sosial yang serius, seperti konflik antarkelompok dan disintegrasi sosial. Oleh karena itu, pengendalian terhadap penyebaran konten ilegal menjadi salah satu fokus utama dalam penegakan hukum siber. Penanganan kejahatan siber memerlukan pendekatan yang berbeda dibandingkan dengan kejahatan konvensional. Aparat penegak hukum harus memiliki kemampuan teknis dalam bidang digital forensic untuk mengumpulkan dan menganalisis bukti elektronik. Selain itu, kerja sama internasional juga sangat penting mengingat banyak kasus cybercrime yang melibatkan pelaku dari berbagai negara (Fariq et al., 2026).

Dengan meningkatnya ketergantungan masyarakat terhadap teknologi informasi, potensi kejahatan siber juga semakin besar. Oleh karena itu, diperlukan upaya yang komprehensif dalam pencegahan dan penanggulangan cybercrime. Upaya tersebut meliputi penguatan regulasi, peningkatan kapasitas penegak hukum, serta edukasi masyarakat mengenai keamanan digital. Tanpa langkah-langkah tersebut, kejahatan siber akan terus berkembang dan menjadi ancaman serius bagi keamanan dan stabilitas masyarakat (Anggreini, 2025; Fariq et al., 2026).

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu suatu pendekatan penelitian hukum yang berfokus pada analisis norma-norma hukum yang berlaku dalam peraturan perundang-undangan serta berbagai sumber hukum lainnya. Metode ini dipilih karena penelitian bertujuan untuk mengkaji bagaimana hukum pidana mengatur dan merespons perkembangan teknologi informasi, khususnya dalam konteks kejahatan siber. Pendekatan yuridis normatif menekankan pada kajian terhadap asas, teori, dan konsep hukum yang relevan sehingga mampu memberikan pemahaman yang komprehensif mengenai permasalahan yang diteliti (Fatur & Ritonga, 2024).

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan hukum pidana dan teknologi informasi, seperti Kitab Undang-Undang Hukum Pidana (KUHP) serta Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Melalui pendekatan ini, penulis dapat mengidentifikasi norma-norma hukum yang berlaku serta menganalisis kesesuaian regulasi tersebut dengan perkembangan teknologi saat ini. Selain itu, pendekatan konseptual digunakan untuk memahami berbagai konsep dan teori yang berkaitan dengan hukum pidana dan teknologi informasi. Pendekatan ini dilakukan dengan mengkaji pendapat para ahli hukum serta teori-teori yang berkembang dalam literatur ilmiah. Dengan demikian, penelitian tidak hanya berfokus pada teks hukum semata, tetapi juga mempertimbangkan aspek filosofis dan teoritis yang mendasari pembentukan hukum tersebut. Pendekatan konseptual ini penting untuk memberikan analisis yang lebih mendalam terhadap permasalahan yang diteliti (Fatur & Ritonga, 2024).

Sumber data dalam penelitian ini merupakan data sekunder yang diperoleh dari berbagai

bahan hukum. Bahan hukum tersebut terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan dengan topik penelitian. Bahan hukum sekunder mencakup buku-buku hukum, jurnal ilmiah, serta hasil penelitian terdahulu yang berkaitan dengan hukum pidana dan teknologi informasi. Sementara itu, bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber lain yang mendukung pemahaman terhadap istilah dan konsep yang digunakan (Fatur & Ritonga, 2024).

Pengumpulan data dilakukan melalui studi kepustakaan (*library research*), yaitu dengan cara menelusuri dan mengkaji berbagai literatur yang relevan dengan topik penelitian. Penelitian ini secara khusus menggunakan sumber dari jurnal ilmiah dan buku elektronik yang diterbitkan dalam rentang tahun 2016–2026 guna memastikan bahwa data yang digunakan sesuai dengan perkembangan terkini. Proses pengumpulan data dilakukan secara sistematis dengan mengelompokkan sumber berdasarkan relevansi dan kualitasnya (Fatur & Ritonga, 2024).

Selanjutnya, data yang telah dikumpulkan dianalisis menggunakan metode analisis kualitatif. Analisis dilakukan dengan menginterpretasikan data yang diperoleh, kemudian menghubungkannya dengan permasalahan yang diteliti. Hasil analisis disajikan secara deskriptif untuk memberikan gambaran yang jelas mengenai perkembangan hukum pidana dalam menghadapi teknologi informasi. Dengan metode ini, diharapkan penelitian dapat menghasilkan kesimpulan yang logis, sistematis, dan dapat dipertanggungjawabkan secara ilmiah (Fariq et al., 2026).

HASIL DAN PEMBAHASAN

Pembahasan terhadap hasil penelitian dan pengujian yang diperoleh disajikan dalam bentuk uraian teoritik, baik secara kualitatif maupun kuantitatif. Hasil percobaan sebaiknya ditampilkan dalam berupa grafik atau pun tabel. Untuk grafik dapat mengikuti format untuk diagram dan gambar. (Times New Roman, size 12, Spacing: before 0 pt; after 0 pt, Line spacing: 1).

1. Perkembangan Hukum Pidana dalam Era Teknologi Informasi

Perkembangan teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam bidang hukum pidana. Transformasi digital yang terjadi secara masif membuat pola kejahatan ikut berubah, dari yang sebelumnya bersifat konvensional menjadi berbasis teknologi. Kejahatan seperti penipuan, pencurian, hingga penyebaran informasi palsu kini dapat dilakukan melalui ruang siber dengan jangkauan yang jauh lebih luas. Kondisi ini menuntut hukum pidana untuk beradaptasi agar tetap relevan dan mampu memberikan perlindungan hukum bagi masyarakat. Hukum pidana konvensional pada dasarnya dirancang untuk mengatur perbuatan yang terjadi secara fisik dan berada dalam batas wilayah tertentu. Namun, dalam konteks kejahatan digital, batasan tersebut menjadi tidak lagi relevan. Kejahatan siber dapat dilakukan lintas negara tanpa kehadiran fisik pelaku di lokasi korban. Hal ini menimbulkan tantangan dalam penentuan yurisdiksi hukum serta penegakan hukum lintas batas negara. Selain itu, identifikasi pelaku kejahatan digital menjadi lebih kompleks dibandingkan kejahatan konvensional. Pelaku dapat dengan mudah menyembunyikan identitasnya melalui berbagai teknologi seperti VPN, akun anonim, atau teknik enkripsi. Hal ini menyulitkan aparat penegak hukum dalam melakukan pelacakan dan pengumpulan bukti yang mengarah pada pelaku. Akibatnya, proses penegakan hukum seringkali membutuhkan waktu yang lebih lama dan sumber daya yang lebih besar (Sautaqi, 2023).

Bukti dalam kejahatan digital juga memiliki karakteristik yang berbeda karena bersifat elektronik. Bukti digital dapat berupa data, log aktivitas, rekaman komunikasi, atau file yang tersimpan dalam perangkat elektronik. Sifatnya yang mudah diubah, dihapus, atau dipindahkan menuntut adanya standar dan metode khusus dalam pengumpulan serta pengamanan bukti. Oleh karena itu, hukum pidana perlu mengatur secara jelas mengenai validitas dan kekuatan pembuktian dari bukti digital. Sebagai respons terhadap perkembangan ini, Indonesia telah mengembangkan regulasi khusus untuk mengatur kejahatan di bidang teknologi informasi. Salah satu regulasi yang paling dikenal adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini menjadi landasan hukum dalam menangani berbagai bentuk kejahatan siber, seperti pencemaran nama baik, penipuan online, hingga akses ilegal terhadap sistem elektronik. Tidak hanya regulasi, aparat penegak hukum juga mulai memanfaatkan teknologi dalam proses penyidikan dan penegakan hukum. Penggunaan digital forensik, analisis data, serta pelacakan jejak digital menjadi bagian penting dalam mengungkap kejahatan siber. Kemampuan ini memungkinkan aparat untuk mengidentifikasi pelaku dan mengumpulkan bukti secara lebih efektif, meskipun kejahatan dilakukan secara virtual (Silalahi & Antonio, 2025)

Namun demikian, perkembangan hukum pidana seringkali tertinggal dibandingkan dengan perkembangan teknologi itu sendiri. Inovasi teknologi yang sangat cepat membuat regulasi yang ada menjadi cepat usang atau tidak lagi memadai. Hal ini menciptakan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan untuk menghindari jerat hukum. Situasi ini menjadi tantangan besar bagi pembuat kebijakan dalam merumuskan regulasi yang adaptif dan responsif. Selain itu, terdapat pula tantangan dalam hal perlindungan hak asasi manusia dalam penegakan hukum digital. Penggunaan teknologi dalam penyidikan, seperti penyadapan atau pengawasan digital, berpotensi melanggar privasi jika tidak diatur dengan ketat. Oleh karena itu, hukum pidana harus mampu menyeimbangkan antara kepentingan penegakan hukum dan perlindungan hak individu. Kerja sama internasional juga menjadi aspek penting dalam perkembangan hukum pidana di era digital. Mengingat kejahatan siber bersifat lintas negara, diperlukan koordinasi antarnegara dalam hal pertukaran informasi, ekstradisi, dan penegakan hukum. Tanpa kerja sama ini, pelaku kejahatan dapat dengan mudah berpindah yurisdiksi untuk menghindari proses hukum. Secara keseluruhan, perkembangan hukum pidana dalam era teknologi informasi merupakan proses yang dinamis dan penuh tantangan. Diperlukan pembaruan regulasi yang berkelanjutan, peningkatan kapasitas aparat penegak hukum, serta kerja sama lintas sektor dan negara. Dengan demikian, hukum pidana dapat tetap berfungsi secara efektif dalam menjaga ketertiban dan keadilan di tengah pesatnya perkembangan teknologi informasi (Kifli, 2025; Silalahi & Antonio, 2025).

2. Bentuk-Bentuk Kejahatan Siber

a. Penipuan Online

Penipuan online merupakan salah satu bentuk kejahatan siber yang paling sering terjadi di Indonesia. Modus yang digunakan pelaku sangat beragam, mulai dari penawaran barang fiktif, investasi bodong, hingga penyamaran sebagai pihak tertentu seperti bank atau marketplace. Kemudahan akses internet dan tingginya aktivitas jual beli secara daring membuat kejahatan ini semakin marak. Dalam praktiknya, pelaku biasanya memanfaatkan platform seperti media sosial, aplikasi pesan instan, dan marketplace untuk menjangkau korban. Mereka sering menggunakan foto produk yang

menarik dan harga yang tidak wajar (terlalu murah) untuk memancing minat calon pembeli. Setelah korban melakukan pembayaran, pelaku kemudian menghilang tanpa mengirimkan barang yang dijanjikan. Selain itu, penipuan online juga sering melibatkan teknik manipulasi psikologis. Pelaku memanfaatkan rasa percaya, panik, atau keserakahan korban agar mengambil keputusan secara cepat tanpa berpikir panjang. Contohnya adalah modus “flash sale palsu” atau penawaran terbatas yang membuat korban merasa harus segera bertindak. Dampak dari penipuan online tidak hanya kerugian materiil, tetapi juga dapat menimbulkan trauma psikologis bagi korban. Banyak korban merasa malu atau takut untuk melapor, sehingga kasus-kasus ini seringkali tidak terungkap secara maksimal. Hal ini juga menjadi tantangan dalam penegakan hukum. Untuk mengatasi masalah ini, diperlukan peningkatan literasi digital masyarakat agar lebih waspada terhadap berbagai modus penipuan. Selain itu, platform digital juga perlu meningkatkan sistem keamanan dan verifikasi penjual untuk meminimalkan potensi kejahatan. Penegakan hukum terhadap pelaku penipuan online juga harus diperkuat dengan dukungan teknologi, seperti pelacakan transaksi digital dan kerja sama dengan lembaga keuangan. Dengan pendekatan yang komprehensif, diharapkan kejahatan ini dapat ditekan (Fariq et al., 2026).

b. Pencurian Data Pribadi

Pencurian data pribadi merupakan kejahatan siber yang semakin meningkat seiring dengan banyaknya aktivitas digital masyarakat. Data pribadi seperti nama, nomor identitas, alamat, nomor telepon, hingga informasi keuangan menjadi target utama pelaku kejahatan. Data ini memiliki nilai ekonomi yang tinggi di pasar gelap digital. Pelaku biasanya memperoleh data melalui berbagai cara, seperti phishing, malware, atau peretasan sistem. Phishing dilakukan dengan cara mengelabui korban agar memberikan informasi sensitif melalui situs atau pesan palsu yang menyerupai institusi resmi. Sementara itu, malware digunakan untuk menyusup ke perangkat korban dan mencuri data secara diam-diam. Setelah data diperoleh, pelaku dapat menyalahgunakannya untuk berbagai kepentingan, seperti penipuan, pemerasan, atau bahkan penjualan data kepada pihak lain. Dalam beberapa kasus, data pribadi juga digunakan untuk membuat akun palsu atau melakukan transaksi ilegal atas nama korban. Dampak dari pencurian data pribadi sangat serius, karena dapat merugikan korban secara finansial maupun reputasi (Sautaqi, 2023).

c. Ujaran Kebencian dan Hoaks

Ujaran kebencian dan hoaks merupakan bentuk kejahatan siber yang berkaitan dengan penyebaran informasi di ruang digital. Ujaran kebencian biasanya ditujukan kepada individu atau kelompok tertentu berdasarkan suku, agama, ras, atau golongan. Sementara itu, hoaks adalah informasi palsu yang disebarkan seolah-olah benar. Perkembangan media sosial menjadi faktor utama yang mempercepat penyebaran ujaran kebencian dan hoaks. Informasi dapat dengan mudah viral dalam waktu singkat tanpa melalui proses verifikasi yang memadai. Hal ini membuat masyarakat rentan terpengaruh oleh informasi yang tidak benar. Motif pelaku dalam menyebarkan hoaks dan ujaran kebencian beragam, mulai dari kepentingan politik, ekonomi, hingga sekadar mencari perhatian. Dalam beberapa kasus, penyebaran informasi palsu dilakukan secara terorganisir untuk mempengaruhi opini public (Santoso et al., 2024).

d. Peretasan Sistem

Peretasan sistem atau hacking merupakan tindakan akses ilegal terhadap sistem komputer atau jaringan tanpa izin. Kejahatan ini dapat dilakukan oleh individu maupun kelompok dengan tujuan tertentu, seperti mencuri data, merusak sistem, atau mengambil alih kendali. Pelaku peretasan biasanya memiliki kemampuan teknis yang tinggi dan memanfaatkan celah keamanan dalam sistem. Mereka dapat menggunakan berbagai metode, seperti brute force attack, SQL injection, atau eksploitasi software yang belum diperbarui. Dalam beberapa kasus, peretasan dilakukan terhadap sistem penting seperti perbankan, perusahaan, atau instansi pemerintah. Hal ini dapat menyebabkan kerugian besar, baik secara finansial maupun operasional. Bahkan, peretasan juga dapat mengganggu stabilitas keamanan nasional. Selain itu, terdapat juga jenis peretasan yang dikenal sebagai ransomware, di mana pelaku mengunci sistem korban dan meminta tebusan untuk mengembalikan akses (Fariq et al., 2026).

3. Efektivitas UU ITE dalam Penegakan Hukum

a. Multiinterpretasi Pasal

Salah satu kritik utama terhadap UU ITE adalah adanya pasal-pasal yang bersifat multitafsir. Ketidakjelasan dalam perumusan norma hukum menyebabkan perbedaan penafsiran baik di kalangan aparat penegak hukum maupun masyarakat. Hal ini menimbulkan ketidakpastian hukum, karena suatu perbuatan dapat dianggap melanggar hukum dalam satu kasus, tetapi tidak dalam kasus lain. Pasal yang paling sering menjadi sorotan adalah pasal terkait pencemaran nama baik. Banyak pihak menilai bahwa batasan antara kritik, opini, dan pencemaran nama baik tidak dijelaskan secara tegas. Akibatnya, masyarakat sering merasa ragu dalam menyampaikan pendapat di ruang digital karena takut terjerat hukum. Selain itu, multitafsir juga membuka peluang terjadinya kriminalisasi terhadap individu. Beberapa kasus menunjukkan bahwa pasal-pasal tertentu digunakan untuk melaporkan pihak yang sebenarnya hanya menyampaikan kritik atau keluhan. Kondisi ini menimbulkan kekhawatiran terhadap kebebasan berekspresi di era digital (Santoso et al., 2024).

b. Penegakan Hukum

Efektivitas UU ITE juga sangat dipengaruhi oleh kemampuan aparat dalam menegakkan hukum di bidang siber. Penegakan hukum kejahatan siber memiliki tantangan yang berbeda dibandingkan kejahatan konvensional, terutama karena melibatkan teknologi yang terus berkembang. Salah satu kendala utama adalah keterbatasan sumber daya manusia yang memiliki keahlian khusus di bidang teknologi informasi. Tidak semua aparat penegak hukum memiliki kemampuan dalam digital forensik atau analisis data, sehingga proses penyidikan seringkali menjadi kurang optimal. Selain itu, keterbatasan infrastruktur dan teknologi juga menjadi hambatan. Penanganan kejahatan siber membutuhkan perangkat dan sistem yang canggih untuk melacak aktivitas digital serta mengamankan bukti elektronik. Tanpa dukungan teknologi yang memadai, proses penegakan hukum menjadi kurang efektif. Masalah lain yang sering muncul adalah sifat kejahatan siber yang lintas wilayah bahkan lintas negara. Hal ini menyulitkan proses penyidikan, terutama jika pelaku berada di luar yurisdiksi Indonesia. Kerja sama internasional menjadi sangat penting, tetapi tidak selalu mudah dilakukan (Kifli, 2025).

c. Perlindungan Data Pribadi

Perlindungan data pribadi menjadi salah satu isu penting dalam konteks penerapan UU ITE. Meskipun telah ada regulasi tambahan yang mengatur

perlindungan data, implementasinya masih menghadapi berbagai kendala di lapangan. Salah satu permasalahan utama adalah masih rendahnya kesadaran masyarakat mengenai pentingnya menjaga data pribadi. Banyak pengguna internet yang dengan mudah membagikan informasi sensitif tanpa mempertimbangkan risiko yang mungkin terjadi. Hal ini membuat data pribadi rentan disalahgunakan. Selain itu, masih terdapat kelemahan dalam sistem keamanan data pada beberapa institusi, baik pemerintah maupun swasta. Kebocoran data yang terjadi dalam beberapa kasus menunjukkan bahwa perlindungan data belum sepenuhnya optimal. Hal ini dapat merugikan masyarakat dalam skala besar (Sautaqi, 2023).

4. Tantangan dalam Hukum Pidana Digital

a. Kecepatan Perkembangan Teknologi

Perkembangan teknologi informasi berlangsung sangat cepat dan sering kali melampaui kemampuan hukum untuk mengikutinya. Inovasi baru seperti kecerdasan buatan, blockchain, dan Internet of Things terus bermunculan dan menciptakan bentuk interaksi baru di ruang digital. Hal ini membuat hukum pidana harus terus beradaptasi agar tetap relevan. Kecepatan perubahan ini menyebabkan regulasi yang ada menjadi cepat usang. Ketika suatu undang-undang disahkan, teknologi yang menjadi objek pengaturannya bisa saja sudah berkembang lebih jauh. Akibatnya, terdapat celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan. Selain itu, perkembangan teknologi juga melahirkan jenis-jenis kejahatan baru yang sebelumnya tidak dikenal. Misalnya, kejahatan berbasis deepfake, pencurian aset digital, atau manipulasi data berbasis kecerdasan buatan. Hukum pidana seringkali belum memiliki definisi atau pengaturan yang jelas terhadap fenomena tersebut (Silalahi & Antonio, 2025).

b. Kurangnya Literasi Digital

Literasi digital masyarakat Indonesia masih tergolong rendah, terutama dalam hal pemahaman terhadap risiko dan keamanan di dunia maya. Banyak pengguna internet yang belum memahami cara melindungi data pribadi atau mengenali potensi kejahatan siber. Kondisi ini membuat masyarakat menjadi sasaran empuk bagi pelaku kejahatan digital. Modus seperti phishing, penipuan online, dan penyebaran hoaks seringkali berhasil karena kurangnya pengetahuan korban. Hal ini menunjukkan bahwa aspek edukasi masih menjadi tantangan besar. Selain itu, rendahnya literasi digital juga berdampak pada perilaku pengguna dalam bermedia sosial. Banyak individu yang tidak menyadari bahwa tindakan mereka, seperti menyebarkan informasi palsu atau ujaran kebencian, dapat memiliki konsekuensi hukum (Sautaqi, 2023).

c. Kerja Sama Internasional

Kejahatan siber memiliki karakter lintas negara, sehingga penanganannya tidak dapat dilakukan secara nasional saja. Pelaku dapat dengan mudah melakukan aksinya dari negara lain, sementara korban berada di Indonesia. Hal ini menuntut adanya kerja sama internasional yang kuat. Namun, dalam praktiknya, kerja sama internasional masih menghadapi berbagai kendala. Perbedaan sistem hukum, prosedur, dan kepentingan antarnegara seringkali menghambat proses penegakan hukum. Tidak semua negara memiliki regulasi yang sejalan dalam menangani kejahatan siber. Selain itu, proses ekstradisi pelaku kejahatan juga tidak selalu mudah dilakukan. Diperlukan perjanjian bilateral atau multilateral yang mengatur mekanisme tersebut. Tanpa adanya

perjanjian, pelaku dapat lolos dari jerat hukum dengan berlindung di negara lain (Fariq et al., 2026).

d. Kompleksitas Pembuktian Digital

Pembuktian dalam kejahatan siber memiliki tingkat kompleksitas yang lebih tinggi dibandingkan kejahatan konvensional. Bukti yang digunakan umumnya bersifat digital, seperti data elektronik, log aktivitas, atau rekaman komunikasi. Salah satu tantangan utama adalah memastikan keaslian dan integritas bukti digital. Bukti tersebut harus dijaga agar tidak mengalami perubahan sejak dikumpulkan hingga diajukan di pengadilan. Hal ini membutuhkan prosedur dan teknologi khusus. Selain itu, proses pengumpulan bukti digital memerlukan keahlian teknis yang tinggi. Aparat penegak hukum harus memahami cara kerja sistem komputer dan jaringan untuk dapat mengidentifikasi serta mengamankan bukti dengan benar (Kifli, 2025).

5. Upaya Pembaruan Hukum

Upaya pembaruan hukum dalam menghadapi tantangan era digital merupakan kebutuhan yang tidak dapat dihindari. Perkembangan teknologi informasi yang sangat pesat telah mengubah pola interaksi masyarakat sekaligus melahirkan berbagai bentuk kejahatan baru. Oleh karena itu, hukum pidana harus terus diperbarui agar tetap relevan, adaptif, dan mampu memberikan kepastian hukum. Pembaruan ini tidak hanya mencakup perubahan regulasi, tetapi juga penguatan sistem penegakan hukum secara menyeluruh. Salah satu langkah utama dalam pembaruan hukum adalah melakukan revisi regulasi secara berkala. Undang-undang yang mengatur kejahatan siber harus mampu mengikuti dinamika teknologi yang terus berkembang. Tanpa pembaruan yang rutin, regulasi akan menjadi usang dan tidak mampu menjangkau bentuk-bentuk kejahatan baru yang muncul di ruang digital. Revisi regulasi juga diperlukan untuk memperjelas norma hukum yang masih bersifat multitafsir. Ketidakjelasan aturan dapat menimbulkan ketidakpastian hukum serta membuka peluang penyalahgunaan kewenangan. Dengan perumusan yang lebih tegas dan rinci, hukum dapat diterapkan secara lebih adil dan konsisten (Santoso et al., 2024).

Selain itu, pembaruan regulasi harus mempertimbangkan keseimbangan antara penegakan hukum dan perlindungan hak asasi manusia. Dalam konteks digital, isu seperti privasi, kebebasan berekspresi, dan perlindungan data pribadi menjadi sangat penting. Oleh karena itu, regulasi yang dibentuk harus mampu melindungi masyarakat tanpa mengorbankan hak-hak dasar individu. Di samping revisi regulasi, penguatan kapasitas aparat penegak hukum menjadi faktor kunci dalam efektivitas hukum pidana digital. Aparat harus memiliki kompetensi yang memadai di bidang teknologi informasi agar mampu menangani kasus kejahatan siber dengan baik. Tanpa keahlian tersebut, penegakan hukum akan mengalami hambatan yang signifikan. Penguatan kapasitas ini dapat dilakukan melalui pelatihan berkelanjutan, pendidikan khusus, serta peningkatan keterampilan di bidang digital forensik. Aparat juga perlu memahami perkembangan teknologi terbaru agar tidak tertinggal dalam menghadapi modus kejahatan yang semakin kompleks. Dengan demikian, proses penyidikan dan pembuktian dapat dilakukan secara lebih efektif (Damayanti, 2026).

Selain sumber daya manusia, dukungan infrastruktur dan teknologi juga sangat penting. Aparat penegak hukum membutuhkan perangkat yang canggih untuk melacak aktivitas digital mengamankan bukti elektronik, dan menganalisis data. Investasi dalam teknologi menjadi bagian penting dari upaya pembaruan hukum. Upaya lainnya adalah meningkatkan edukasi masyarakat tentang literasi digital. Masyarakat yang memiliki

pemahaman yang baik tentang teknologi akan lebih mampu melindungi diri dari kejahatan siber. Literasi digital tidak hanya mencakup kemampuan teknis, tetapi juga pemahaman tentang etika dan hukum dalam penggunaan teknologi. Edukasi ini dapat dilakukan melalui berbagai jalur, seperti pendidikan formal, kampanye publik, maupun pelatihan berbasis komunitas. Dengan meningkatnya kesadaran masyarakat, potensi kejahatan siber dapat ditekan karena masyarakat menjadi lebih waspada dan tidak mudah menjadi korban. Terakhir, kerja sama internasional menjadi elemen penting dalam pembaruan hukum pidana digital. Mengingat kejahatan siber bersifat lintas negara, diperlukan koordinasi antarnegara dalam penanganannya. Kerja sama ini mencakup pertukaran informasi, ekstradisi pelaku, serta harmonisasi regulasi. Secara keseluruhan, upaya pembaruan hukum harus dilakukan secara komprehensif dan berkelanjutan. Kombinasi antara revisi regulasi, penguatan aparat, edukasi masyarakat, dan kerja sama internasional akan menciptakan sistem hukum yang lebih tangguh dalam menghadapi tantangan era digital. Dengan demikian, hukum pidana dapat tetap berfungsi secara efektif dalam menjaga keamanan dan keadilan di tengah perkembangan teknologi (Silalahi & Antonio, 2025; Fariq et al., 2026).

KESIMPULAN

Perkembangan hukum pidana di Indonesia menunjukkan adanya upaya adaptasi terhadap kemajuan teknologi informasi, terutama melalui pembentukan dan revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Regulasi ini menjadi instrumen penting dalam mengatur berbagai aktivitas di ruang digital sekaligus memberikan dasar hukum dalam penindakan kejahatan siber. Namun demikian, perkembangan tersebut masih belum sepenuhnya mampu mengimbangi laju inovasi teknologi yang sangat cepat. Hal ini terlihat dari masih adanya kekosongan hukum, multitafsir norma, serta keterbatasan dalam menjangkau bentuk-bentuk kejahatan digital yang terus berkembang. Selain itu, efektivitas hukum pidana dalam menangani kejahatan siber masih menghadapi berbagai kendala yang cukup kompleks. Kendala tersebut meliputi aspek regulasi yang belum sepenuhnya komprehensif, keterbatasan kapasitas aparat penegak hukum dalam bidang teknologi, serta rendahnya tingkat kesadaran dan literasi digital masyarakat. Kondisi ini menunjukkan bahwa penanganan kejahatan siber tidak hanya bergantung pada keberadaan hukum semata, tetapi juga memerlukan sinergi antara regulasi yang adaptif, penegakan hukum yang profesional, serta partisipasi aktif masyarakat dalam menciptakan lingkungan digital yang aman.

DAFTAR REFERENSI

- Agustian, A. (2021). Tindak pidana informasi elektronik dalam kerangka hukum positif. *PROGRESIF: Jurnal Hukum*, 1(1), 92–111.
- Anggreini, B. (2025). Penguatan hukum pidana Indonesia dalam menghadapi kejahatan siber era digital. *Journal Terekam Jejak (JTJ)*, 3(3), 8–20.
- Damayanti, P. N. (2026). Analisis perkembangan hukum teknologi informasi dan kaitannya terhadap penetapan tersangka Roy Suryo Notodiprojo Cs. *Ranah Research: Journal of Multidisciplinary Research and Development*, 8(2), 1188–1194.
- Fariq, D. Al, Sitanggang, R. M., Putra, R. S., & Khairunnisa, C. (2026). Perbandingan hukum pidana dalam penanganan kejahatan teknologi informasi antara Indonesia dan Singapura. *ULIL ALBAB: Jurnal Ilmiah Multidisiplin*, 5(5), 559–568.
- Fatur, A., & Ritonga, R. (2024). Pengaruh digitalisasi proses hukum acara pidana: Studi komparatif hukum Indonesia dan Thailand (*Criminal Procedure Code*). *Jurnal Ilmiah Penelitian LAW*

- JURNAL*, 5(2), 83–94.
- Kifli, S. (2025). Penegakan hukum pidana di Indonesia terhadap kejahatan siber di era digital. *Jurnal Ilmu Hukum The Juris*, 9(1), 182–188.
- Republik Indonesia. (1946). *Kitab Undang-Undang Hukum Pidana (KUHP)*.
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Republik Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*.
- Santoso, I., Syahrin, A., & Mulyadi, M. (2024). Kebijakan hukum pidana terhadap perbuatan melawan hukum dalam UU ITE pasca berlakunya pedoman implementasi pasal-pasal tertentu UU ITE. *Locus Journal of Academic Literature Review*, 3(4), 329–335.
- Sutaqi, I. M. (2023). Dampak perkembangan teknologi terhadap hukum sebagai tantangan dimensi baru keamanan siber. *Juncto Delictio*, 3(1), 47–54.
- Silalahi, W., & Antonio, M. L. (2025). Reformasi hukum acara penyidikan di era digital: Analisis kesesuaian KUHAP dan KUHP baru terhadap kebutuhan teknologi informasi dalam perspektif ketatanegaraan. *Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi*, 2(4), 121–133.