Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

PENERAPAN HUKUM PIDANA TERHADAP PELAKU TINDAK PIDANA SIBER DI INDONESIA: ANALISIS PUTUSAN PENGADILAN

APPLICATION OF CRIMINAL LAW TOWARDS PERPETRATORS OF CYBER CRIMES IN INDONESIA: ANALYSIS OF COURT DECISIONS

Agus Siagian[1]*, Dony Alexander[2]
Universitas Batam, Indonesia[1], Universitas Islam Sultan Agung, Indonesia[2]
Email: siagian.agus76@gmail.com[1]*, donyalexander513@gmail.com[2]

Abstract

This study aims to analyze how criminal law is applied to perpetrators of cybercrime in Indonesia through a review of several court decisions. With the increasing use of information technology, cybercrime has become a serious challenge in the criminal justice system. This study uses a normative juridical method with a qualitative approach through literature review and content analysis of court decisions. The results show that the types of cybercrime predominantly handled through the courts include online fraud, defamation, hate speech, and the distribution of illegal content. The application of criminal law by judges is carried out by referring to articles in the Criminal Code and the ITE Law, despite inconsistencies in interpretation and technical obstacles in electronic evidence. Judges' considerations in issuing decisions include aspects of legality, justice, and the social impact of the crime. However, there remains a gap between the ideal principles of justice and legal certainty and the reality of practice in the field. This study recommends harmonization of regulations, increasing the capacity of law enforcement officers, and strengthening jurisprudence as steps to improve law enforcement against cybercrime.

Keywords: Cyber Crime, Criminal Law, ITE Law, Court Decisions, Justice and Legal Certainty.

Abstrak

Penelitian ini bertujuan untuk menganalisis bagaimana hukum pidana diterapkan terhadap pelaku tindak pidana siber di Indonesia melalui kajian terhadap sejumlah putusan pengadilan. Seiring dengan meningkatnya penggunaan teknologi informasi, kejahatan siber menjadi tantangan serius dalam sistem hukum pidana. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan kualitatif melalui studi pustaka dan analisis isi putusan pengadilan. Hasil penelitian menunjukkan bahwa jenis kejahatan siber yang dominan ditangani melalui pengadilan meliputi penipuan daring, pencemaran nama baik, ujaran kebencian, dan penyebaran konten ilegal. Penerapan hukum pidana oleh hakim dilakukan dengan mengacu pada pasal-pasal dalam KUHP dan UU ITE, meskipun terdapat ketidakkonsistenan interpretasi dan kendala teknis dalam pembuktian elektronik. Pertimbangan hakim dalam menjatuhkan putusan meliputi aspek legalitas, keadilan, dan dampak sosial dari tindak pidana. Namun demikian, masih terdapat celah antara asas keadilan dan kepastian hukum yang ideal dengan realitas praktik di lapangan. Penelitian ini merekomendasikan harmonisasi regulasi, peningkatan kapasitas aparat penegak hukum, dan penguatan yurisprudensi sebagai langkah perbaikan dalam penegakan hukum terhadap kejahatan siber.

Kata kunci: Tindak Pidana Siber, Hukum Pidana, UU ITE, Putusan Pengadilan, Keadilan dan Kepastian Hukum.

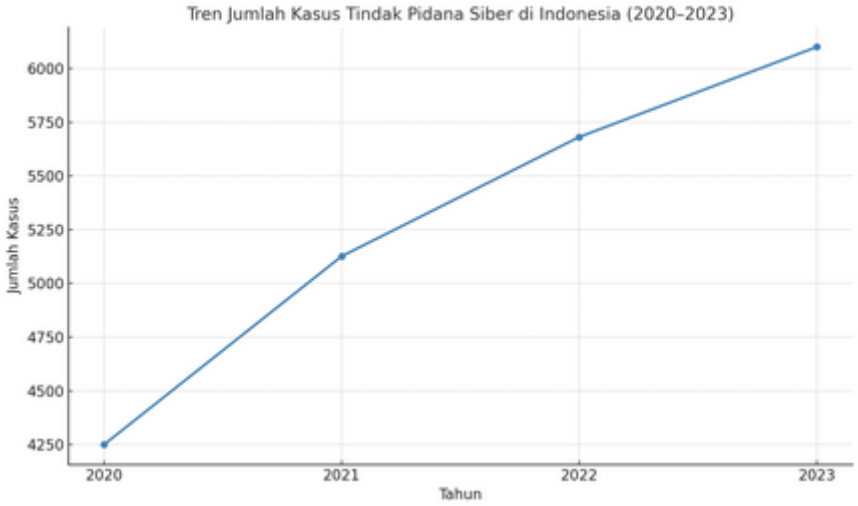
PENDAHULUAN

Dalam era digital yang terus berkembang pesat, penggunaan teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari masyarakat. Transformasi digital yang menyentuh hampir seluruh aspek kehidupan, mulai dari komunikasi, perdagangan, hingga sistem pemerintahan, telah membawa banyak manfaat. Namun, perkembangan ini juga

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

melahirkan tantangan baru, salah satunya adalah munculnya tindak pidana siber (cyber crime). Kejahatan siber mencakup berbagai bentuk pelanggaran hukum yang dilakukan melalui atau terhadap sistem teknologi informasi dan komunikasi, seperti peretasan (hacking), pencurian data, penipuan daring (online fraud), penyebaran hoaks, hingga penyalahgunaan media sosial.

Di Indonesia, kejahatan siber menunjukkan tren peningkatan baik dalam jumlah maupun kompleksitasnya. Hal ini menuntut adanya respons hukum yang cepat, tepat, dan efektif dari aparat penegak hukum. Pemerintah Indonesia telah merespons fenomena ini dengan menerbitkan berbagai regulasi, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diubah dengan UU No. 19 Tahun 2016. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) juga tetap digunakan untuk menjerat pelaku kejahatan siber yang memenuhi unsur-unsur delik umum. Meski demikian, penerapan hukum pidana terhadap pelaku tindak pidana siber sering kali menghadapi tantangan, baik dalam aspek pembuktian, yurisdiksi, maupun ketepatan penafsiran pasal-pasal hukum yang relevan.



Gambar 1. Jumlah kasus tindak pidana siber

Gambar di atas memperlihatkan data tren jumlah kasus tindak pidana siber di Indonesia berdasarkan laporan Direktorat Tindak Pidana Siber, Bareskrim Polri. Pada tahun 2020, tercatat sebanyak 4.250 kasus, yang kemudian meningkat menjadi 5.126 kasus pada tahun 2021. Tren ini terus berlanjut dengan 5.681 kasus pada tahun 2022, hingga mencapai sekitar 6.100 kasus pada tahun 2023. Peningkatan jumlah kasus ini menunjukkan bahwa kejahatan siber menjadi tantangan serius bagi sistem hukum pidana nasional. Bentuk kejahatan yang dilaporkan mencakup penipuan daring, ujaran kebencian, penyebaran hoaks, penghinaan di media sosial, serta penyalahgunaan data pribadi. Fenomena ini dipicu oleh meningkatnya penggunaan internet dan media sosial, minimnya literasi digital, serta lemahnya perlindungan data pribadi.

Peningkatan jumlah kasus setiap tahun mencerminkan urgensi perbaikan dalam sistem penegakan hukum pidana, termasuk dalam hal pembuktian digital, sinkronisasi regulasi

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

(KUHP dan UU ITE), serta konsistensi putusan pengadilan. Data ini juga menjadi landasan penting dalam melakukan analisis terhadap bagaimana hukum pidana diterapkan terhadap pelaku kejahatan siber di Indonesia, khususnya melalui studi terhadap putusan-putusan pengadilan. Tantangan tersebut menjadi semakin kompleks ketika persoalan yuridis bertemu dengan konteks sosial-politik tertentu. Tidak sedikit putusan pengadilan terhadap pelaku tindak pidana siber yang menimbulkan kontroversi, baik karena dianggap tidak adil, tidak proporsional, atau bahkan mengandung tafsir hukum yang multitafsir. Oleh karena itu, penting untuk melakukan analisis terhadap putusan-putusan pengadilan dalam perkara siber guna memahami bagaimana hukum pidana diterapkan secara konkret di lapangan, serta sejauh mana asas keadilan dan kepastian hukum dapat ditegakkan.

Penelitian ini memiliki urgensi yang tinggi mengingat perkembangan kejahatan siber di Indonesia semakin mengkhawatirkan dari tahun ke tahun. Fenomena digitalisasi yang merambah seluruh aspek kehidupan tidak hanya membawa kemudahan, tetapi juga membuka ruang baru bagi munculnya tindak pidana dengan modus yang semakin kompleks dan sulit dideteksi. Kejahatan siber tidak lagi bersifat lokal, melainkan lintas batas, dan sering kali sulit dibuktikan secara hukum konvensional. Dalam konteks ini, sistem hukum pidana nasional dituntut untuk mampu merespons dinamika tersebut secara adaptif dan progresif. Urgensi penelitian ini juga terletak pada masih banyaknya perdebatan dan ketidakpastian dalam penerapan hukum pidana terhadap pelaku kejahatan siber, khususnya dalam hal penggunaan pasal-pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP). Banyak putusan pengadilan yang dinilai tidak konsisten, baik dari segi dasar hukum, pertimbangan yuridis, maupun jenis dan beratnya hukuman yang dijatuhkan. Ketidakkonsistenan ini tidak hanya menimbulkan kebingungan di kalangan aparat penegak hukum, tetapi juga berpotensi melanggar prinsip keadilan dan kepastian hukum bagi masyarakat.

Selain itu, perlindungan terhadap hak-hak korban dan pelaku tindak pidana siber juga masih menjadi persoalan serius. Dalam beberapa kasus, pelaku dijatuhi hukuman berat meskipun perbuatannya masih dapat ditafsirkan secara multitafsir. Di sisi lain, banyak korban kejahatan siber yang belum mendapatkan keadilan karena lemahnya pembuktian dan lambatnya proses hukum. Oleh karena itu, penelitian ini menjadi penting sebagai upaya untuk mengkaji bagaimana hukum pidana diterapkan secara nyata terhadap pelaku kejahatan siber melalui analisis terhadap putusan-putusan pengadilan. Seiring meningkatnya kasus tindak pidana siber di Indonesia, sejumlah penelitian telah dilakukan untuk menganalisis aspek hukum terkait cyber crime, baik dari sisi normatif, perbandingan hukum, hingga kebijakan publik. Misalnya, penelitian oleh Handayani (2018) menyoroti problematika penafsiran pasal-pasal dalam UU ITE yang dianggap multitafsir dan berpotensi mengancam kebebasan berekspresi.

Sementara itu, Putra dan Rachmad (2019) mengkaji kesesuaian pasal pidana dalam KUHP terhadap fenomena penipuan daring, namun belum menggambarkan praktik penerapan hukumnya di tingkat peradilan. Rasyid dan Azzahra (2020) meneliti efektivitas sanksi pidana dalam kasus ujaran kebencian di media sosial, tetapi fokus mereka masih

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

terbatas pada aspek teori hukum dan belum menyentuh aspek empiris berupa analisis putusan pengadilan. Lebih lanjut, Astari (2021) melakukan studi terhadap kebijakan penegakan hukum terhadap kejahatan digital, namun pendekatan yang digunakan masih deskriptif normatif dan belum menguji secara konkret bagaimana hakim menafsirkan dan menerapkan hukum pidana dalam perkara siber. Begitu pula dengan Prasetya dan Lestari (2022) yang meneliti perlindungan hukum terhadap korban kejahatan digital, tetapi tidak menelaah bagaimana struktur peradilan mengakomodasi prinsip keadilan dalam putusan terhadap pelaku.

Dari telaah berbagai studi tersebut, terlihat adanya kekosongan (gap) dalam kajian yang secara langsung menganalisis putusan pengadilan sebagai objek utama untuk memahami penerapan hukum pidana terhadap pelaku kejahatan siber. Kebanyakan studi masih berfokus pada aspek normatif atau teoretis, dan belum secara mendalam mengevaluasi argumentasi yuridis dalam putusan, konsistensi antar putusan, dan relevansi hukum yang digunakan dalam menjatuhkan hukuman terhadap pelaku. Padahal, putusan pengadilan merupakan manifestasi paling konkret dari pelaksanaan hukum pidana dalam sistem peradilan. Dengan latar belakang tersebut, penelitian ini akan membahas penerapan hukum pidana terhadap pelaku tindak pidana siber di Indonesia melalui analisis terhadap putusan pengadilan. Penelitian ini bertujuan untuk menggali bagaimana argumentasi hukum dibangun oleh hakim, bagaimana proses penegakan hukum berlangsung, serta menilai konsistensi dan efektivitas penerapan hukum pidana dalam menghadapi fenomena kejahatan siber yang semakin berkembang. Melalui pendekatan ini, diharapkan dapat memberikan kontribusi terhadap pengembangan sistem hukum pidana nasional yang lebih responsif terhadap dinamika kejahatan digital.

Perkembangan teknologi informasi dan komunikasi telah melahirkan bentuk-bentuk kejahatan baru yang dikenal sebagai tindak pidana siber (cyber crime). Kejahatan jenis ini tidak hanya kompleks secara teknis, tetapi juga sering menimbulkan permasalahan dalam penerapan hukum pidana yang berlaku. Salah satu permasalahan utama adalah bagaimana aparat penegak hukum, khususnya hakim, menerapkan pasal-pasal hukum yang relevan dalam menjatuhkan putusan terhadap pelaku kejahatan siber. Terdapat sejumlah kasus di mana penerapan pasal dalam UU ITE maupun KUHP dipertanyakan keabsahannya karena multitafsir atau tidak tepat sasaran.

Selain itu, proses pembuktian dalam kasus siber cenderung lebih sulit dibanding kejahatan konvensional karena keterbatasan alat bukti digital, lokasi pelaku yang bisa lintas wilayah bahkan lintas negara, serta keterbatasan kapasitas penyidik dan penuntut umum. Keadaan ini berdampak pada kualitas putusan pengadilan yang beragam: ada yang tegas dan jelas, tetapi ada pula yang menimbulkan kontroversi, baik dari aspek yuridis maupun dari sisi keadilan substantif.

Permasalahan lain yang turut muncul adalah sejauh mana hukum pidana yang digunakan—baik bersumber dari KUHP maupun UU ITE—telah mampu menjawab tantangan dan kompleksitas kejahatan siber. Apakah hakim memiliki dasar pertimbangan

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

yang cukup kuat dalam menjatuhkan vonis terhadap pelaku? Apakah ada konsistensi antara satu putusan dengan putusan lainnya untuk kasus yang sejenis?

Berangkat dari latar belakang tersebut, perlu dilakukan identifikasi lebih lanjut terhadap bagaimana hukum pidana diterapkan terhadap pelaku kejahatan siber di Indonesia, khususnya melalui pendekatan analisis putusan pengadilan sebagai cerminan penerapan hukum yang konkret dan final.

Berdasarkan identifikasi permasalahan di atas, maka rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana bentuk dan jenis tindak pidana siber yang ditangani melalui mekanisme peradilan pidana di Indonesia?
2. Bagaimana hakim menerapkan hukum pidana (KUHP dan/atau UU ITE) dalam memutus perkara tindak pidana siber?
3. Apa saja pertimbangan hukum yang digunakan dalam menjatuhkan putusan terhadap pelaku tindak pidana siber?
4. Sejauh mana putusan pengadilan terhadap pelaku tindak pidana siber mencerminkan asas keadilan dan kepastian hukum?
5. Apa saja kendala yang dihadapi dalam proses penegakan hukum pidana terhadap kejahatan siber di Indonesia berdasarkan analisis putusan?

TINJAUAN PUSTAKA

Teori Hukum Pidana

Hukum pidana merupakan cabang hukum publik yang mengatur perbuatan-perbuatan yang dilarang oleh negara dan diancam dengan sanksi pidana bagi siapa saja yang melanggarnya. Dalam konteks ini, hukum pidana memiliki dua fungsi utama: sebagai sarana pengendalian sosial (social control) dan sebagai perlindungan terhadap kepentingan hukum masyarakat. Menurut Moeljatno (2002), hukum pidana terdiri dari norma-norma hukum yang mengatur larangan dan kewajiban, serta disertai ancaman sanksi bagi yang melanggar.

Dalam penerapannya, hukum pidana harus memenuhi unsur-unsur tertentu, yaitu adanya perbuatan yang melawan hukum, kesalahan atau culpa dari pelaku, dan ancaman pidana yang ditentukan dalam peraturan perundang-undangan. Dalam kasus kejahatan siber, tantangan besar muncul karena bentuk kejahatannya tidak selalu bisa dijelaskan dengan pendekatan hukum pidana konvensional. Oleh karena itu, penegak hukum harus mengadaptasi asas-asas hukum pidana dalam menanggapi kejahatan digital yang berkembang pesat.

Teori Pemidanaan

Teori pemidanaan berkaitan erat dengan tujuan dari pemberian hukuman kepada pelaku kejahatan. Terdapat beberapa teori dalam pemidanaan, yaitu teori absolut (pembalasan), teori relatif (pencegahan), dan teori gabungan. Dalam teori absolut, pidana diberikan sebagai pembalasan atas perbuatan jahat yang dilakukan. Sedangkan teori relatif melihat pidana sebagai sarana untuk mencegah kejahatan, baik secara umum (dengan

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

menakut-nakuti masyarakat) maupun khusus (mencegah pelaku mengulangi perbuatannya). Teori gabungan mencoba memadukan nilai-nilai pembalasan dengan pencegahan demi kepentingan keadilan dan ketertiban hukum.

Dalam kasus tindak pidana siber, hakim dihadapkan pada persoalan bagaimana menjatuhkan pidana yang sebanding dan adil, terutama ketika pelaku adalah pengguna awam teknologi yang mungkin tidak sepenuhnya memahami dampak perbuatannya. Di sinilah pentingnya pemahaman teori pemidanaan sebagai dasar pertimbangan hakim dalam menyusun amar putusan.

Teori Penegakan Hukum

Teori penegakan hukum sebagaimana dikemukakan oleh Satjipto Rahardjo (2006) menekankan bahwa hukum tidak semata-mata berbentuk aturan tertulis, tetapi juga harus berpihak pada keadilan substantif. Penegakan hukum tidak hanya dilakukan melalui pendekatan normatif, melainkan harus mempertimbangkan nilai-nilai keadilan, moralitas, dan kemanusiaan. Penegakan hukum dalam konteks kejahatan siber membutuhkan fleksibilitas dan kepekaan terhadap perubahan sosial, karena karakteristik pelaku dan modus kejahatan kerap kali berada dalam wilayah yang abu-abu secara hukum.

Dalam banyak kasus siber, pelaku mungkin belum pernah memiliki catatan kriminal, dan korban kadang tidak menyadari dampak langsung dari peristiwa tersebut. Oleh sebab itu, proses penegakan hukum membutuhkan kehati-hatian agar tidak menimbulkan kriminalisasi yang berlebihan, namun tetap menjamin kepastian hukum dan rasa keadilan masyarakat.

Teori Kejahatan Siber *(Cybercrime)*

Cybercrime merupakan bentuk kejahatan yang memanfaatkan teknologi informasi dan sistem digital sebagai sarana atau objek kejahatan. Menurut Thomas dan Loader (2000), kejahatan siber meliputi aktivitas ilegal yang dilakukan melalui jaringan komputer atau terhadap sistem informasi yang dilindungi. Kejahatan ini bersifat lintas batas (borderless), real-time, dan sulit dideteksi, sehingga memerlukan pendekatan hukum yang lebih canggih dibanding kejahatan konvensional.

Beberapa karakteristik utama kejahatan siber antara lain: (1) sulitnya mengidentifikasi pelaku secara fisik; (2) kerugian tidak selalu bersifat material langsung; dan (3) alat bukti yang digunakan berbentuk digital, yang mudah dimodifikasi atau dihapus. Dengan demikian, penerapan hukum pidana terhadap kejahatan siber tidak hanya memerlukan pemahaman tentang norma hukum, tetapi juga pemahaman teknis dan forensik digital.

Kerangka Pemikiran

Dari berbagai teori yang telah diuraikan di atas, dapat disusun suatu kerangka pemikiran bahwa penerapan hukum pidana terhadap pelaku kejahatan siber harus memperhatikan tiga aspek utama:

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

1. Aspek normatif, yaitu kejelasan dan kesesuaian norma hukum yang digunakan (UU ITE, KUHP).
2. Aspek yuridis-empiris, yakni bagaimana putusan hakim dibentuk, dipertimbangkan, dan dijatuhkan.
3. Aspek keadilan, yaitu sejauh mana pidana yang dijatuhkan sesuai dengan prinsip keadilan, baik bagi korban, pelaku, maupun masyarakat secara umum.

Melalui analisis putusan pengadilan, penelitian ini berupaya menguji sejauh mana teori-teori hukum pidana di atas benar-benar tercermin dalam praktik peradilan terhadap pelaku kejahatan siber.

METODE

Penelitian ini merupakan penelitian hukum normatif-empiris yang memadukan pendekatan doktrinal (normatif) dengan studi lapangan melalui analisis dokumen yuridis. Penelitian hukum normatif digunakan untuk menelaah norma-norma hukum positif yang berlaku terkait tindak pidana siber, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP). Sementara itu, pendekatan empiris dilakukan dengan menganalisis putusan pengadilan sebagai objek konkret dari penerapan hukum pidana.

Pendekatan ini bertujuan untuk memahami bagaimana hakim dalam praktiknya menafsirkan dan menerapkan hukum pidana terhadap pelaku kejahatan siber, serta menilai konsistensi, rasionalitas, dan keadilannya. Dengan demikian, penelitian ini bersifat eksploratif dan analitis, berusaha mengungkap hubungan antara norma hukum, pelaksanaan peradilan, dan nilai keadilan substantif.

Pengumpulan data dilakukan dengan cara:

1) Studi kepustakaan (library research) untuk menggali teori-teori dan konsep hukum pidana, teori pemidanaan, serta teori kejahatan siber yang menjadi kerangka konseptual dalam penelitian ini.
2) Studi dokumen (documentary study) terhadap salinan putusan pengadilan yang dianalisis secara sistematis. Dokumen ini menjadi sumber utama dalam menilai bagaimana hukum diterapkan dalam praktik peradilan.
3) Pengumpulan data daring, khususnya melalui basis data Mahkamah Agung dan JDIH (Jaringan Dokumentasi dan Informasi Hukum) sebagai sumber hukum positif.

Data dianalisis dengan menggunakan metode analisis isi (content analysis) terhadap putusan pengadilan yang diteliti. Analisis ini dilakukan dengan menelaah:

1) Identitas perkara dan pihak terkait
2) Pasal yang digunakan dalam penuntutan dan putusan
3) Argumentasi hukum hakim (pertimbangan yuridis dan filosofis)
4) Jenis dan berat pidana yang dijatuhkan
5) Kesesuaian putusan dengan asas hukum pidana (lex certa, lex scripta, dan asas legalitas)
6) Keadilan dan kepastian hukum dalam konteks penerapan pidana

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

Analisis dilakukan secara kualitatif, yaitu dengan menarik kesimpulan berdasarkan pola, konsistensi, dan kecenderungan dalam beberapa putusan yang diteliti. Hasil analisis ini akan menjadi dasar untuk menjawab rumusan masalah dan menarik simpulan substantif dari penelitian.

HASIL DAN PEMBAHASAN

Bagaimana Bentuk dan Jenis Tindak Pidana Siber yang Ditangani Melalui Mekanisme Peradilan Pidana di Indonesia

Perkembangan teknologi informasi telah melahirkan bentuk-bentuk kejahatan baru yang berbeda secara karakteristik dari kejahatan konvensional. Kejahatan yang menggunakan atau menyerang sistem elektronik dan jaringan komputer ini dikenal sebagai tindak pidana siber (cybercrime). Di Indonesia, tindak pidana siber mulai memperoleh perhatian serius seiring dengan meningkatnya jumlah kasus yang ditangani oleh aparat penegak hukum, serta dampaknya yang signifikan terhadap ketertiban umum, ekonomi, hingga reputasi individu dan institusi. Mekanisme penyelesaiannya sebagian besar dilakukan melalui sistem peradilan pidana, baik berdasarkan KUHP, UU ITE, maupun peraturan pendukung lainnya.

Tabel 1. Regulasi yang Mendasari Penerapan Hukum Pidana Siber

Nama Regulasi	Isi Pokok	Keterangan
UU No. 11 Tahun 2008 tentang ITE	Mengatur informasi dan transaksi elektronik, termasuk pelanggaran yang dilakukan melalui media digital	Diubah dengan UU No. 19 Tahun 2016
KUHP Pasal 310–311	Penghinaan dan pencemaran nama baik	Sering dijadikan dasar dalam kasus siber
KUHP Pasal 378	Penipuan	Digunakan dalam kasus penipuan daring
Peraturan Kapolri No. 6 Tahun 2019	Penyidikan Tindak Pidana	Menjelaskan tata cara penanganan perkara termasuk siber

Bentuk tindak pidana siber yang paling banyak ditangani dalam praktik peradilan di Indonesia meliputi penipuan daring (online fraud), pencemaran nama baik melalui media elektronik, ujaran kebencian (hate speech), penyebaran berita bohong (hoaks), akses ilegal ke sistem elektronik (hacking), penyebaran konten asusila, dan penyalahgunaan data pribadi. Kasus-kasus tersebut umumnya dijerat menggunakan Pasal 27, Pasal 28, dan Pasal 29 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan UU No. 19 Tahun 2016, serta ketentuan pasal dalam KUHP seperti Pasal 310–311 (pencemaran nama baik), Pasal 378 (penipuan), dan Pasal 156a (penghinaan terhadap agama).

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

Misalnya, dalam kasus penipuan berbasis e-commerce, pelaku biasanya menawarkan barang fiktif melalui media sosial atau platform digital dan menerima pembayaran tanpa mengirimkan barang. Jenis kejahatan ini paling banyak terjadi dan telah diadili dalam ratusan perkara di pengadilan negeri. Dalam kasus pencemaran nama baik, pelaku menyebarkan tuduhan atau fitnah terhadap seseorang melalui Facebook, Instagram, atau WhatsApp, yang mengakibatkan kerugian non-material seperti hilangnya nama baik atau gangguan psikologis. Sementara itu, kasus ujaran kebencian dan penyebaran hoaks meningkat tajam terutama menjelang momentum politik seperti pemilu, di mana konten bermuatan provokasi atau disinformasi tersebar secara masif. Selain kejahatan terhadap individu, terdapat pula tindak pidana siber yang menyerang sistem negara dan kepentingan umum, seperti hacking terhadap situs pemerintah atau penyebaran malware. Meskipun jenis ini lebih sedikit dalam jumlah, ancamannya tergolong tinggi karena menyangkut kerahasiaan data dan stabilitas keamanan nasional. Penanganannya memerlukan dukungan teknis dari instansi seperti Badan Siber dan Sandi Negara (BSSN) dan sering kali masuk ke dalam kategori kejahatan transnasional.

Dalam proses peradilan, bentuk-bentuk tindak pidana siber ini ditangani dengan pendekatan konvensional, yaitu melalui proses penyidikan oleh kepolisian, penuntutan oleh kejaksaan, dan pemeriksaan di pengadilan. Tantangan utama dalam penanganannya terletak pada pengumpulan alat bukti elektronik, identifikasi pelaku yang sering menggunakan nama samaran atau akun palsu, serta keterbatasan pemahaman hakim terhadap isu teknis digital. Meski demikian, beberapa putusan pengadilan menunjukkan bahwa bentuk-bentuk kejahatan siber telah secara konsisten masuk dalam wilayah yuridis pidana, dengan hukuman yang bervariasi tergantung jenis dan dampak dari kejahatan tersebut. Dengan demikian, dapat disimpulkan bahwa mekanisme peradilan pidana di Indonesia telah menangani berbagai bentuk dan jenis kejahatan siber yang semakin kompleks, meskipun masih menghadapi kendala teknis dan yuridis. Keragaman bentuk kejahatan ini menunjukkan perlunya pembaruan dan penguatan kapasitas lembaga peradilan agar mampu menanggapi dinamika kejahatan di era digital secara lebih efektif dan adil.

Bagaimana Hakim Menerapkan Hukum Pidana (KUHP dan/atau UU ITE) dalam Memutus Perkara Tindak Pidana Siber

Dalam sistem peradilan pidana Indonesia, hakim memiliki peran sentral sebagai pihak yang memberikan penilaian akhir atas suatu perbuatan pidana, termasuk tindak pidana siber. Penerapan hukum pidana terhadap pelaku kejahatan siber dilakukan berdasarkan kombinasi antara Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah melalui UU Nomor 19 Tahun 2016. Dalam praktiknya, hakim akan terlebih dahulu menilai jenis kejahatan yang dilakukan dan pasal mana yang paling relevan untuk diterapkan sesuai dengan fakta hukum yang terungkap di persidangan. Hakim tidak serta-merta menerapkan seluruh pasal dalam UU ITE atau KUHP, tetapi melakukan konstruksi hukum berdasarkan unsur-unsur delik yang dibuktikan dalam persidangan. Misalnya, dalam kasus pencemaran

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

nama baik melalui media sosial, hakim akan mengacu pada Pasal 27 ayat (3) UU ITE, yang mensyaratkan adanya distribusi dan/atau transmisi informasi elektronik yang bermuatan penghinaan atau pencemaran nama baik. Dalam hal ini, hakim menilai apakah unggahan atau pesan elektronik tersebut memang bermuatan pencemaran, apakah pelaku dapat diidentifikasi, serta apakah unsur "kesengajaan" terpenuhi.

Jika suatu kasus tidak dapat secara tepat dikualifikasikan dalam pasal-pasal UU ITE, hakim dapat menggunakan pasal-pasal pidana umum dalam KUHP. Sebagai contoh, Pasal 378 KUHP tentang penipuan sering digunakan bersama Pasal 28 ayat (1) UU ITE dalam kasus penipuan daring, di mana pelaku menyebarkan informasi palsu dengan tujuan untuk memperoleh keuntungan pribadi secara melawan hukum. Dalam beberapa putusan, hakim menggabungkan dasar hukum dari kedua undang-undang tersebut untuk memperkuat legitimasi putusan dan memberikan dasar pidana yang lebih komprehensif. Dalam pertimbangannya, hakim juga mengacu pada alat bukti digital, seperti tangkapan layar, rekaman percakapan elektronik, alamat IP, serta keterangan ahli digital forensik. Ini merupakan bentuk penyesuaian dalam pembuktian tindak pidana siber, di mana barang bukti konvensional seperti saksi langsung sering kali tidak tersedia. Selain itu, hakim turut mempertimbangkan niat jahat (mens rea) dan akibat dari perbuatan tersebut, apakah telah menyebabkan kerugian nyata atau sekadar berpotensi menimbulkan keresahan publik.

Namun, tidak semua penerapan hukum pidana dalam kasus siber berjalan ideal. Dalam sejumlah kasus, penerapan pasal oleh hakim menuai kritik karena dianggap multitafsir atau digunakan untuk membungkam ekspresi publik. Misalnya, Pasal 27 ayat (3) UU ITE kerap digunakan terhadap kritik di media sosial, yang secara substansi lebih dekat ke delik perdata atau pelanggaran etika, bukan pidana. Hal ini menunjukkan bahwa penerapan hukum oleh hakim masih menghadapi tantangan dalam menyeimbangkan antara perlindungan hukum, hak kebebasan berekspresi, dan keadilan. Di sisi lain, ada pula kasus-kasus di mana hakim dengan baik menegakkan hukum pidana terhadap pelaku yang terbukti meretas sistem pemerintahan atau menyebarkan konten pornografi melalui internet. Dalam perkara-perkara seperti ini, hakim secara tegas menerapkan sanksi pidana yang mencerminkan seriusnya ancaman dari kejahatan siber terhadap ketertiban umum dan moralitas publik.

Secara keseluruhan, penerapan hukum pidana oleh hakim dalam perkara kejahatan siber menunjukkan adanya upaya untuk menyesuaikan pendekatan hukum dengan karakteristik dunia digital. Meski demikian, perbedaan tafsir, kompleksitas alat bukti, serta dinamika sosial-politik sering kali mempengaruhi arah dan hasil putusan. Oleh karena itu, dibutuhkan peningkatan pemahaman para hakim terhadap hukum siber serta pembaruan regulasi agar penerapan hukum lebih konsisten, adil, dan kontekstual.

Apa Saja Pertimbangan Hukum yang Digunakan dalam Menjatuhkan Putusan Terhadap Pelaku Tindak Pidana Siber

Dalam menjatuhkan putusan terhadap pelaku tindak pidana siber, hakim tidak hanya berpegang pada teks undang-undang secara normatif, tetapi juga mempertimbangkan berbagai aspek yuridis, sosiologis, dan filosofis. Hal ini penting mengingat kejahatan siber

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

memiliki karakteristik yang unik, baik dari segi modus operandi, dampak terhadap korban, maupun tantangan pembuktian. Oleh karena itu, pertimbangan hukum yang digunakan hakim harus mampu menjawab kompleksitas tersebut secara adil dan proporsional. Pertimbangan hukum yang pertama dan paling utama adalah pemenuhan unsur-unsur delik yang tertuang dalam pasal yang digunakan oleh jaksa penuntut umum dalam dakwaan. Misalnya, jika pelaku didakwa berdasarkan Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik, maka hakim akan menilai apakah perbuatan terdakwa memenuhi unsur-unsur seperti adanya transmisi informasi elektronik, isi informasi yang bersifat menyerang kehormatan atau nama baik orang lain, serta adanya niat (mens rea) dalam perbuatan tersebut. Pemenuhan unsur ini menjadi dasar objektif dalam penjatuhan putusan.

Kedua, hakim juga mempertimbangkan alat bukti yang sah menurut hukum acara pidana, yang dalam konteks siber sering kali berupa bukti digital. Alat bukti ini bisa berupa tangkapan layar (screenshot), riwayat percakapan digital, log server, atau keterangan ahli digital forensik. Dalam banyak kasus, hakim akan menilai keabsahan dan keandalan bukti digital tersebut, termasuk bagaimana proses perolehannya—apakah dilakukan sesuai prosedur hukum atau melanggar asas due process of law. Jika bukti tidak sah atau diperoleh secara melawan hukum, maka hakim dapat mengesampingkan bukti tersebut meskipun isinya tampak memberatkan terdakwa. Ketiga, dalam perkara siber, hakim juga memperhatikan pertimbangan sosiologis, yakni sejauh mana perbuatan terdakwa telah merugikan pihak lain, menimbulkan keresahan publik, atau membahayakan kepentingan umum. Misalnya, dalam kasus penyebaran hoaks yang menimbulkan kepanikan, pertimbangan dampak sosial menjadi sangat relevan. Hakim dalam hal ini berusaha menjaga keseimbangan antara kepentingan individu (terdakwa) dan kepentingan masyarakat luas.

Selanjutnya, hakim juga mempertimbangkan faktor-faktor yang meringankan atau memberatkan hukuman. Faktor yang meringankan bisa berupa usia muda pelaku, penyesalan terdakwa, belum pernah dihukum sebelumnya, atau adanya perdamaian dengan korban. Sementara itu, faktor yang memberatkan bisa mencakup perbuatan dilakukan secara berulang, menggunakan identitas palsu, mengakibatkan kerugian besar, atau dilakukan terhadap kelompok rentan (seperti anak-anak dalam kasus pornografi online). Pertimbangan ini menjadi dasar untuk menentukan berat-ringannya pidana yang dijatuhkan, seperti pidana penjara, denda, atau pidana tambahan. Tidak kalah penting, hakim juga merujuk pada yurisprudensi atau putusan sebelumnya yang relevan, guna menjaga konsistensi dalam penerapan hukum. Dalam banyak putusan, hakim mencantumkan referensi dari perkara serupa sebagai pembanding dan penguat argumentasi hukum. Ini menunjukkan bahwa hakim tidak bertindak sewenang-wenang, tetapi berada dalam kerangka sistem hukum yang berkesinambungan.

Di sisi lain, dalam konteks kejahatan siber yang melibatkan ekspresi di ruang digital, seperti kritik terhadap pejabat publik atau aktivisme daring, hakim juga diharapkan mempertimbangkan aspek hak asasi manusia, khususnya kebebasan berekspresi sebagaimana dijamin oleh UUD 1945 dan berbagai instrumen internasional yang telah diratifikasi Indonesia. Hal ini penting agar tidak terjadi kriminalisasi terhadap warga negara

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

yang menyuarakan pendapat secara damai. Dengan berbagai pertimbangan tersebut, terlihat bahwa hakim tidak hanya bertindak sebagai pelaksana undang-undang secara tekstual, tetapi juga sebagai penafsir yang harus adil dan bijak dalam menghadapi dinamika perkembangan masyarakat digital. Putusan yang dijatuhkan harus tidak hanya memenuhi aspek legalitas, tetapi juga mencerminkan keadilan substantif dan memberi efek jera bagi pelaku serta perlindungan bagi masyarakat.

Sejauh Mana Putusan Pengadilan Terhadap Pelaku Tindak Pidana Siber Mencerminkan Asas Keadilan dan Kepastian Hukum

Putusan pengadilan merupakan wujud konkret dari pelaksanaan hukum dalam menyelesaikan suatu perkara. Dalam konteks tindak pidana siber di Indonesia, putusan pengadilan tidak hanya diuji dari segi formalnya, tetapi juga sejauh mana ia mencerminkan asas keadilan dan kepastian hukum sebagai pilar utama dalam sistem peradilan pidana. Kejahatan siber yang terus berkembang dengan cepat menuntut sistem hukum, termasuk hakim, untuk menafsirkan dan menerapkan hukum secara adaptif tanpa mengorbankan prinsip dasar hukum itu sendiri. Secara normatif, asas kepastian hukum menuntut agar hukum ditegakkan secara konsisten, tidak berubah-ubah, dan dapat diprediksi. Dalam banyak kasus kejahatan siber, hakim berupaya menegakkan kepastian hukum dengan merujuk langsung pada ketentuan yang terdapat dalam UU ITE maupun KUHP, serta memastikan bahwa unsur-unsur pidana dalam dakwaan terpenuhi secara jelas dan terperinci. Kepastian hukum tercermin ketika hakim menggunakan pasal-pasal yang tepat dan menghindari multitafsir terhadap perbuatan yang dilakukan terdakwa, misalnya dengan membedakan antara kritik dan ujaran kebencian, atau antara pencemaran nama baik dan hak kebebasan berekspresi.

Namun, di sisi lain, tantangan terhadap kepastian hukum muncul akibat masih belum sempurnanya norma dalam UU ITE, yang mengandung beberapa pasal karet seperti Pasal 27 ayat (3) dan Pasal 28 ayat (2), yang cenderung multitafsir. Akibatnya, dalam beberapa putusan pengadilan, penegakan hukum justru dinilai mengancam kebebasan sipil karena menggunakan pasal-pasal tersebut untuk menjerat pelaku secara berlebihan. Dalam kasus seperti ini, putusan pengadilan justru dinilai mencederai kepastian hukum karena tidak memberikan perlindungan hukum yang seimbang antara pelaku dan korban, maupun antara negara dan warga negara. Dari perspektif asas keadilan, hakim dituntut untuk memperhatikan konteks sosial, niat pelaku (mens rea), dampak yang ditimbulkan, serta keseimbangan antara hak-hak pelaku dan korban. Dalam perkara-perkara siber yang melibatkan peretasan, penipuan online, penyebaran konten pornografi, atau manipulasi data, keadilan tampak ketika hakim tidak hanya menjatuhkan pidana berdasarkan kerugian material, tetapi juga menimbang dampak psikologis, potensi kerugian jangka panjang, serta motif pelaku. Di sisi lain, dalam kasus-kasus yang cenderung mengandung unsur kritik terhadap kekuasaan, asas keadilan mengharuskan hakim untuk tidak serta-merta menghukum pelaku, melainkan mempertimbangkan hak konstitusional atas kebebasan berekspresi.

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

Dalam praktiknya, tidak semua putusan pengadilan secara utuh mencerminkan keadilan. Beberapa putusan dinilai lebih mengedepankan legalitas formal ketimbang substansi keadilan. Misalnya, ketika seorang warga yang menyuarakan kritik melalui media sosial dihukum pidana penjara karena dianggap mencemarkan nama baik, padahal kritik tersebut dilindungi oleh prinsip demokrasi dan kebebasan berpendapat. Dalam kasus demikian, keadilan substantif menjadi kabur karena hukum digunakan sebagai alat represi, bukan perlindungan. Namun demikian, terdapat juga putusan-putusan yang menunjukkan upaya hakim dalam menjaga keseimbangan antara asas keadilan dan kepastian hukum. Misalnya, hakim dalam beberapa kasus siber mulai mempertimbangkan penggunaan restorative justice, terutama untuk pelaku yang masih di bawah umur atau pelanggaran yang pertama kali dilakukan. Ini menunjukkan bahwa hakim tidak hanya menjadi pelaksana hukum secara mekanis, tetapi juga berperan sebagai penjaga moral dan sosial yang mempertimbangkan dampak jangka panjang dari kriminalisasi.

Secara keseluruhan, dapat disimpulkan bahwa sejauh ini putusan pengadilan terhadap pelaku tindak pidana siber di Indonesia masih berada pada titik dinamis antara keinginan menegakkan kepastian hukum dan tuntutan memenuhi keadilan substantif. Konsistensi putusan, kualitas pertimbangan hakim, serta sensitivitas terhadap konteks sosial sangat menentukan sejauh mana dua asas ini dapat ditegakkan secara bersamaan. Oleh karena itu, evaluasi terhadap putusan-putusan pengadilan dan penyempurnaan norma hukum menjadi hal yang mutlak untuk memperkuat kualitas sistem peradilan pidana siber di Indonesia.

Apa Saja Kendala yang Dihadapi dalam Proses Penegakan Hukum Pidana Terhadap Kejahatan Siber di Indonesia Berdasarkan Analisis Putusan

Penegakan hukum terhadap tindak pidana siber di Indonesia menghadapi berbagai tantangan yang kompleks, baik secara normatif, institusional, maupun teknis. Berdasarkan analisis terhadap sejumlah putusan pengadilan yang menangani kasus-kasus siber seperti penipuan online, pencemaran nama baik digital, ujaran kebencian, peretasan, hingga penyebaran konten ilegal, tampak bahwa kendala-kendala tersebut berkontribusi pada inkonsistensi penegakan hukum dan kurang optimalnya perlindungan hukum bagi masyarakat.

1. *Ketidakjelasan dan multitafsirnya norma hukum (Pasal-Pasal Karet)*
   Salah satu kendala utama adalah masih adanya pasal-pasal dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya pasal-pasal seperti Pasal 27 ayat (3) (pencemaran nama baik) dan Pasal 28 ayat (2) (ujaran kebencian), yang dinilai memiliki tafsir yang terlalu luas dan rentan digunakan untuk membungkam kritik. Dalam banyak putusan, hakim memiliki beban untuk menafsirkan sendiri batas antara kritik, penghinaan, dan ujaran kebencian—sebuah hal yang sangat kontekstual dan tidak mudah ditentukan secara objektif. Hal ini mengakibatkan inkonsistensi putusan antar kasus yang serupa.
2. *Keterbatasan aparat penegak hukum dalam aspek teknis dan digital forensic*

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

Penegakan hukum pidana terhadap kejahatan siber sangat bergantung pada kemampuan aparat dalam melakukan investigasi digital. Namun, analisis putusan menunjukkan bahwa dalam banyak kasus, penyidikan dan pembuktian tidak dilengkapi dengan alat bukti digital yang kuat. Aparat penegak hukum kerap mengalami kesulitan dalam menelusuri jejak digital, menyita data elektronik, dan mengekstrak bukti dari perangkat teknologi yang digunakan pelaku. Keterbatasan ini membuat beberapa kasus tidak dapat dilanjutkan ke tahap penuntutan atau gagal dibuktikan di pengadilan.

3. *Kurangnya sinkronisasi antara KUHP dan UU ITE*
   Sebagian besar putusan menunjukkan bahwa penuntutan terhadap kejahatan siber kadang dilakukan secara bersamaan berdasarkan KUHP dan UU ITE. Namun, tidak adanya sinkronisasi antara kedua peraturan tersebut sering kali membingungkan majelis hakim dalam menetapkan dasar hukum yang tepat. Misalnya, dalam kasus ujaran kebencian, apakah pelaku harus dijerat dengan Pasal 156a KUHP atau Pasal 28 ayat (2) UU ITE, sering menjadi perdebatan di persidangan.
4. *Perlindungan terhadap hak konstitusional warga negara*
   Putusan-putusan pengadilan juga memperlihatkan adanya ketegangan antara penegakan hukum dan perlindungan terhadap kebebasan berekspresi. Banyak terdakwa yang divonis karena menyampaikan pendapat di media sosial, padahal kontennya bersifat kritik atau sarkasme terhadap pemerintah atau tokoh publik. Hal ini menimbulkan pertanyaan apakah sistem peradilan pidana telah cukup mengakomodasi prinsip-prinsip hak asasi manusia yang dijamin dalam UUD 1945 dan instrumen internasional.
5. *Kurangnya pemahaman masyarakat terhadap norma hukum digital*
   Banyak kasus kejahatan siber yang muncul akibat minimnya literasi digital masyarakat, baik dari sisi pelaku maupun korban. Beberapa pelaku tidak memahami bahwa tindakan seperti menyebarkan video, memanipulasi informasi, atau mencuri akun media sosial adalah tindak pidana. Di sisi lain, masyarakat juga masih sering melakukan pelaporan secara reaktif, tanpa memahami substansi hukum yang berlaku. Putusan pengadilan sering kali menunjukkan bahwa pelaporan dilakukan karena faktor emosi atau tekanan sosial, bukan berdasarkan pelanggaran hukum yang kuat.
6. *Terbatasnya jurisprudensi yang kuat dan mapan*
   Karena kejahatan siber merupakan fenomena baru yang terus berkembang, banyak hakim masih menghadapi kesulitan dalam merujuk pada yurisprudensi yang stabil. Dalam banyak putusan, tidak ada acuan yuridis yang konsisten sehingga setiap hakim menggunakan pendekatan yang berbeda-beda terhadap kasus yang mirip. Akibatnya, terjadi ketimpangan dalam penjatuhan sanksi dan interpretasi hukum yang membingungkan bagi pelaku maupun masyarakat.

PENUTUP

Kesimpulan

Berdasarkan hasil penelitian dan analisis terhadap sejumlah putusan pengadilan dalam perkara tindak pidana siber, dapat disimpulkan beberapa hal sebagai berikut:

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

1. Tindak pidana siber di Indonesia telah ditangani melalui mekanisme peradilan pidana, baik dengan dasar hukum KUHP maupun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Jenis kejahatan siber yang banyak ditangani meliputi penipuan daring, ujaran kebencian, pencemaran nama baik, penyebaran konten ilegal, dan akses ilegal terhadap sistem elektronik.
2. Hakim dalam memutus perkara siber cenderung menggunakan kombinasi pasal dari KUHP dan UU ITE, dengan pertimbangan fakta hukum, alat bukti elektronik, serta penilaian terhadap niat dan akibat perbuatan terdakwa. Namun, masih ditemukan ketidakkonsistenan penerapan pasal dan variasi pemaknaan atas unsur delik.
3. Pertimbangan hukum dalam menjatuhkan putusan tidak hanya didasarkan pada aspek legalitas, tetapi juga mempertimbangkan keadilan, efek jera, kondisi sosial terdakwa, serta dampak terhadap korban. Dalam beberapa kasus, hakim juga memperhatikan hak atas kebebasan berekspresi yang dilindungi konstitusi.
4. Putusan pengadilan terhadap pelaku tindak pidana siber belum sepenuhnya mencerminkan asas keadilan dan kepastian hukum, terutama karena masih adanya multitafsir pasal dalam UU ITE, lemahnya pembuktian elektronik, serta kurangnya rujukan yurisprudensi yang mapan.
5. Beberapa kendala utama dalam penegakan hukum pidana terhadap kejahatan siber meliputi keterbatasan teknis dalam penyidikan digital, tumpang tindih norma hukum, lemahnya literasi digital masyarakat, serta ketidaksiapan aparat penegak hukum dalam mengikuti dinamika teknologi.

Saran

1. Perlu dilakukan revisi dan harmonisasi regulasi hukum pidana terkait kejahatan siber, khususnya UU ITE dan KUHP, agar lebih jelas, tidak multitafsir, dan tidak menimbulkan ketimpangan dalam penerapannya di pengadilan.
2. Meningkatkan kapasitas sumber daya manusia di bidang penegakan hukum digital, terutama dalam hal keahlian forensik digital, penyidikan siber, dan pemahaman terhadap perangkat hukum internasional.
3. Mahkamah Agung perlu menyusun pedoman atau yurisprudensi tetap dalam menangani tindak pidana siber, guna menciptakan konsistensi putusan dan menjamin kepastian hukum bagi semua pihak.
4. Mendorong perlindungan terhadap hak-hak konstitusional warga negara seperti kebebasan berekspresi, dengan tetap mengedepankan prinsip proporsionalitas dan keadilan dalam menilai perbuatan siber sebagai delik pidana.
5. Meningkatkan literasi digital dan kesadaran hukum masyarakat, agar warga negara memahami batasan dan konsekuensi hukum dari aktivitas di ruang digital, serta dapat menjadi bagian dari masyarakat digital yang bertanggung jawab.

DOI: https://doi.org/10.54443/sibatik.v4i9.3360

DAFTAR PUSTAKA

Ali, M. (2021). *Teori dan Praktik Pemidanaan dalam Hukum Pidana Indonesia*. Surabaya: LaksBang Press.

Astari, L. D. (2021). Kebijakan Penegakan Hukum terhadap Kejahatan Siber di Indonesia. *Jurnal Kriminologi Indonesia*, 17(1), 73–86.

Handayani, D. (2018). Problematika Penerapan Pasal UU ITE terhadap Ekspresi di Media Sosial. *Jurnal Hukum & HAM*, 9(2), 135–148.

Kitab Undang-Undang Hukum Pidana (KUHP).

Marbun, A. (2019). Cyber Crime dan Penegakan Hukum di Indonesia. *Jurnal Hukum Progresif*, 11(1), 85–97.

Moeljatno. (2002). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

Prasetya, A., & Lestari, V. (2022). Perlindungan Hukum terhadap Korban Kejahatan Digital di Era Industri 4.0. *Jurnal Hukum dan Teknologi*, 3(2), 90–104.

Putra, R. Y., & Rachmad, A. (2019). Kesesuaian Sanksi Pidana dalam KUHP terhadap Kejahatan Penipuan Online. *Jurnal Yustisia*, 8(1), 45–58.

Putusan Mahkamah Agung Republik Indonesia (2020–2023). Database Putusan Perkara Tindak Pidana Siber. Diakses dari: https://putusan3.mahkamahagung.go.id

Rahardjo, S. (2006). *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing.

Rasyid, M., & Azzahra, N. (2020). Efektivitas Sanksi Pidana terhadap Ujaran Kebencian di Media Sosial Berdasarkan UU ITE. *Jurnal Hukum Media*, 12(3), 221–234.

Thomas, D., & Loader, B. (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.

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