JOURNAL OF
LAW, SOCIAL SCIENCE, AND
MANAGEMENT REVIEW
E-ISSN 3064-6006

Kajian Terhadap Pertanggungjawaban Pidana Pelaku Kejahatan Siber (Cybercrime) Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

A Criminal Study Responsibility Of Cybercrime Perpetrators According To Law Number 11 Of 2008 Concerning Electronic Information and Transactions

Wahyu Dwi Saputra [1)]; Desy Maryani [2)]; Sandi Aprianto [3)]
[1,2,3)] ***Universitas Dehasen Bengkulu***
Email: [1)] Wahyu.dwi@gmail.com ;[2)] Desy.maryani@unived.ac.id ;[3)] Sandiapriyanto@gmail.com

How to Cite :
Saputra. W. D., Maryani. D., Apriyanto. S.. (2026). Kajian Terhadap Pertanggungjawaban Pidana Pelaku Kejahatan Siber (Cybercrime) Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Journal of Law, Social Science, and Management Review. 2(3).

ARTICLE HISTORY
Received [25 Februari 2026]
Revised [10 Mei 2026]
Accepted [13 Mei 2026]

KEYWORDS
Accountability, Cyber, Cybercrime.

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan terhadap kehidupan masyarakat, khususnya dengan munculnya berbagai bentuk kejahatan siber (cybercrime). Kejahatan siber memiliki karakteristik yang berbeda dengan kejahatan konvensional, antara lain dilakukan melalui sistem elektronik, bersifat lintas batas negara, serta menggunakan data dan informasi digital sebagai sarana maupun objek kejahatan. Kondisi tersebut menuntut adanya pengaturan hukum pidana yang mampu memberikan kepastian hukum dan perlindungan terhadap kepentingan hukum masyarakat di ruang siber. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) hadir sebagai instrumen hukum untuk mengatur perbuatan pidana di bidang teknologi informasi, termasuk pengaturan mengenai pertanggungjawaban pidana pelaku kejahatan siber. Penelitian ini bertujuan untuk mengkaji pengaturan pertanggungjawaban pidana pelaku kejahatan siber menurut UU ITE serta menganalisis kendala yang dihadapi dalam penerapannya. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Bahan hukum yang digunakan meliputi bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa pengaturan pertanggungjawaban pidana dalam UU ITE pada prinsipnya telah berlandaskan asas kesalahan (geen straf zonder schuld) dan mengakui subjek hukum yang luas, termasuk orang perseorangan dan korporasi. UU ITE juga telah mengatur berbagai bentuk tindak pidana siber beserta sanksi pidananya. Namun demikian, dalam praktik penegakan hukum masih ditemukan berbagai kendala, antara lain kesulitan pembuktian berbasis bukti elektronik, keterbatasan kapasitas aparat penegak hukum, karakter kejahatan siber yang bersifat transnasional, serta potensi multitafsir dalam beberapa ketentuan UU ITE. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta penguatan kerja sama internasional dan literasi digital masyarakat guna mewujudkan penegakan hukum pidana siber yang efektif dan berkeadilan..

ABSTRACT

The development of information and communication technology has had a significant impact on people's lives, particularly with the emergence of various forms of cybercrime. Cybercrime has characteristics that differ from conventional crime, including being committed through electronic systems, being cross-border, and using digital data and information as both a means and object of the crime. These conditions demand the existence of criminal law regulations that can provide legal certainty and

protect the legal interests of the community in cyberspace. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is present as a legal instrument to regulate criminal acts in the field of information technology, including regulations regarding the criminal liability of perpetrators of cybercrime. This study aims to examine the provisions on criminal liability of perpetrators of cybercrime under the ITE Law and analyze the obstacles faced in its implementation. The research method used is normative legal research with a statutory approach, a conceptual approach, and a case approach. The legal materials used include primary, secondary, and tertiary legal materials analyzed qualitatively. The research results show that the provisions on criminal liability in the ITE Law are fundamentally based on the principle of fault (geen straf zonder schuld) and recognize a broad range of legal subjects, including individuals and corporations. The ITE Law also regulates various forms of cybercrime and their associated criminal sanctions. However, in practice, various obstacles remain, including the difficulty of obtaining electronic evidence, the limited capacity of law enforcement officials, the transnational nature of cybercrime, and the potential for multiple interpretations of several provisions of the ITE Law. Therefore, regulatory strengthening, capacity building of law enforcement officials, and strengthening international cooperation and public digital literacy are needed to achieve effective and equitable cybercrime law enforcement..

PENDAHULUAN

Perkembangan teknologi informasi pada era globalisasi telah membawa dampak yang sangat signifikan terhadap kehidupan manusia. Teknologi internet, khususnya, telah menjadi bagian integral dalam berbagai sektor, seperti ekonomi, pendidikan, pemerintahan, hingga aktivitas sosial masyarakat sehari-hari. Internet bukan lagi sekadar sarana komunikasi, tetapi juga menjadi ruang baru (cyberspace) yang membuka peluang luas bagi inovasi, perdagangan, dan interaksi global.

Namun, perkembangan ini juga diikuti oleh munculnya permasalahan hukum baru berupa kejahatan siber (Cybercrime). Cybercrime dapat diartikan sebagai segala bentuk kejahatan yang dilakukan dengan menggunakan komputer, jaringan komputer, atau sistem elektronik sebagai sarana maupun sasaran. Bentuknya beragam, mulai dari peretasan (hacking), penyebaran virus komputer, pencurian identitas (identity theft), penipuan daring (online fraud), perjudian online, hingga penyebaran konten ilegal seperti pornografi anak maupun ujaran kebencian (hate speech).

Cybercrime atau kejahatan siber merupakan istilah yang relatif baru dalam kajian hukum pidana. Secara umum, Cybercrime dapat diartikan sebagai setiap perbuatan melawan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, atau sistem elektronik, baik sebagai alat, sasaran, maupun tempat terjadinya tindak pidana.

Kejahatan siber telah menjadi perhatian global karena sifatnya yang lintas batas (transnational crime). Banyak kasus Cybercrime melibatkan pelaku, korban, dan sistem yang berada di negara berbeda, sehingga penanggulangannya memerlukan instrumen hukum internasional. Instrumen internasional paling penting adalah Convention on Cybercrime (Budapest Convention) 2001, yang digagas oleh Dewan Eropa. Konvensi ini mengatur:

a) Standar hukum pidana terkait akses ilegal, penyalahgunaan perangkat, pemalsuan komputer, dan kejahatan berbasis konten.
b) Prosedur hukum acara khusus untuk penanganan bukti elektronik.
c) Kerja sama internasional dalam penyidikan dan penuntutan kejahatan siber.

Meski Indonesia belum meratifikasi Konvensi Budapest, prinsip-prinsipnya sering dijadikan acuan dalam pembaruan hukum nasional. Selain itu, ada pula resolusi Perserikatan Bangsa-Bangsa (PBB) melalui *United Nations Office on Drugs and Crime* (UNODC) yang mendorong negara-negara untuk memperkuat legislasi dan kerja sama internasional dalam melawan Cybercrime.

Di Indonesia, perkembangan Cybercrime sangat pesat seiring dengan meningkatnya jumlah pengguna internet. Fenomena kejahatan siber di Indonesia mulai dikenal pada akhir 1990-an, ketika akses internet mulai digunakan secara luas. Pada masa itu, bentuk kejahatan siber masih terbatas, seperti peretasan (hacking) terhadap situs-situs pemerintah maupun swasta, serta penyebaran virus komputer sederhana. Salah satu kasus awal yang sempat menghebohkan adalah peretasan situs-situs pemerintah oleh kelompok hacker Indonesia yang kemudian melahirkan komunitas underground dunia maya, seperti “IndoXploit” dan “Jember Hacker Team”. Kejahatan siber pada periode ini lebih banyak didorong oleh motif eksistensi, unjuk kemampuan teknis, atau sekadar iseng.

Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2023 mencapai lebih dari 215 juta jiwa, atau sekitar 78% dari total populasi. Angka ini mencerminkan potensi ekonomi digital yang besar, tetapi sekaligus memperlihatkan meningkatnya kerentanan terhadap tindak kejahatan di ruang siber. Berbagai kasus Cybercrime di Indonesia telah menimbulkan kerugian ekonomi, sosial, bahkan ancaman terhadap keamanan nasional.
Jenis Cybercrime yang marak di Indonesia antara lain:
a. Penipuan daring (online fraud), seperti kasus investasi bodong, penipuan toko online, dan phishing.
b. Peretasan akun media sosial untuk pencemaran nama baik, pemerasan, atau penipuan.
c. Pencurian data pribadi melalui malware atau rekayasa sosial (social engineering).
d. Kejahatan perbankan elektronik, seperti skimming ATM dan pembobolan mobile banking.
e. Penyebaran konten ilegal, termasuk pornografi anak, ujaran kebencian, hingga hoaks politik.

Beberapa kasus besar menggambarkan seriusnya ancaman Cybercrime di Indonesia, antara lain:
a. Kasus pembobolan kartu kredit internasional oleh hacker Indonesia (2000-an) yang merugikan banyak pihak dan menjadikan Indonesia salah satu “sarang carder” di Asia.
b. Kasus ransomware WannaCry (2017) yang melumpuhkan sejumlah sistem rumah sakit dan perusahaan di Indonesia.
c. Kasus kebocoran data pribadi (2020–2022), termasuk data pelanggan e-commerce, layanan kesehatan, hingga data Dukcapil, yang memperlihatkan lemahnya perlindungan data.
d. Kasus judi online yang melonjak pada 2022–2024, di mana ribuan situs diidentifikasi beroperasi secara ilegal, melibatkan jaringan transnasional.

Kemudian, untuk menghadapi tantangan tersebut, negara memiliki kewajiban melindungi masyarakat melalui perangkat hukum. Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan tonggak penting dalam sejarah hukum Indonesia, karena undang-undang ini menjadi dasar hukum pertama yang secara khusus mengatur mengenai aktivitas di dunia siber. UU ITE kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016 untuk menyempurnakan beberapa ketentuan yang dianggap multitafsir dan menyesuaikan dengan perkembangan teknologi informasi yang semakin kompleks.

Salah satu aspek penting dalam UU ITE adalah mengenai pertanggungjawaban pidana bagi pelaku kejahatan siber. Dalam hukum pidana, pertanggungjawaban pidana (criminal liability) merupakan prinsip dasar yang menentukan apakah seseorang dapat dimintai pertanggungjawaban atas perbuatan yang dilakukannya. Secara umum, seseorang dapat dipidana apabila memenuhi unsur perbuatan pidana (actus reus) dan kesalahan (mens rea). Namun, dalam konteks Cybercrime, mekanisme pertanggungjawaban pidana tidak selalu sederhana. Modus operandi kejahatan siber sering kali melibatkan teknologi canggih, bersifat lintas batas negara (transnational crime), menggunakan identitas anonim, dan memanfaatkan kelemahan sistem elektronik. Hal ini menimbulkan tantangan dalam pembuktian, identifikasi pelaku, hingga penegakan hukum.

LANDASAN TEORI

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan fundamental dalam pola interaksi sosial, ekonomi, dan hukum di masyarakat. Transformasi tersebut melahirkan ruang baru yang dikenal sebagai cyberspace atau ruang siber, yaitu ruang virtual tempat berlangsungnya aktivitas manusia melalui sistem elektronik dan jaringan internet. Seiring dengan itu, muncul pula berbagai bentuk perbuatan melawan hukum yang dilakukan dengan memanfaatkan teknologi tersebut, yang kemudian dikenal dengan istilah kejahatan siber (cybercrime).

Secara konseptual, cybercrime merupakan bentuk kejahatan yang memiliki karakteristik khusus karena berkaitan erat dengan penggunaan komputer, sistem elektronik, dan jaringan digital. Barda Nawawi Arief menyatakan bahwa cybercrime adalah tindak pidana yang dilakukan dengan menggunakan komputer dan/atau jaringan komputer, baik sebagai sarana, sasaran, maupun sebagai tempat terjadinya kejahatan. Definisi ini menegaskan bahwa teknologi informasi tidak hanya berfungsi sebagai alat bantu, melainkan menjadi bagian inheren dari terjadinya tindak pidana itu sendiri.

Dalam literatur hukum pidana modern, cybercrime sering dipahami sebagai bentuk new dimension of crime, yakni kejahatan yang berkembang akibat perubahan struktur sosial dan teknologi. Namun demikian, tidak semua cybercrime merupakan kejahatan yang sepenuhnya baru. Sebagian besar cybercrime pada hakikatnya merupakan kejahatan konvensional yang mengalami transformasi dalam modus operandi, dari yang semula dilakukan secara fisik menjadi dilakukan melalui media elektronik. Penipuan, pencemaran nama baik, pemerasan, dan ancaman adalah contoh tindak pidana klasik yang kini banyak dilakukan melalui platform digital dan media sosial.

Perbedaan utama antara kejahatan konvensional dan kejahatan siber terletak pada sarana, ruang, serta dampak kejahatan. Kejahatan siber bersifat lintas batas (borderless), anonim, dan memiliki potensi penyebaran yang sangat cepat. Karakteristik ini menimbulkan tantangan serius dalam penegakan hukum, khususnya terkait penentuan yurisdiksi, pembuktian unsur kesalahan, serta identifikasi pelaku. Oleh karena itu, cybercrime memerlukan pendekatan hukum pidana yang adaptif dan responsif terhadap perkembangan teknologi.

Dalam konteks hukum positif Indonesia, istilah cybercrime tidak didefinisikan secara eksplisit dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Meskipun demikian, keberadaan norma-norma larangan dan ketentuan pidana dalam UU ITE menunjukkan bahwa pembentuk undang-undang secara implisit mengakui cybercrime sebagai kategori tindak pidana tersendiri yang memiliki karakteristik khusus dibandingkan dengan tindak pidana umum dalam KUHP.

UU ITE mengonstruksikan cybercrime melalui perumusan delik-delik yang berkaitan dengan perbuatan “mendistribusikan”, “mentransmisikan”, “membuat dapat diaksesnya”, serta “mengakses tanpa hak” informasi elektronik dan/atau sistem elektronik. Rumusan tersebut mencerminkan bahwa cybercrime dalam perspektif UU ITE berfokus pada penyalahgunaan sistem elektronik yang berdampak pada pelanggaran hak, kepentingan hukum, dan ketertiban umum. Dengan demikian, cybercrime dalam UU ITE dapat dipahami sebagai setiap perbuatan melawan hukum yang dilakukan dengan menggunakan sistem elektronik dan menimbulkan akibat hukum pidana sebagaimana diatur dalam undang-undang tersebut.

Dari sudut pandang teori hukum pidana, cybercrime tetap tunduk pada asas-asas umum hukum pidana, khususnya asas legalitas dan asas kesalahan (geen straf zonder schuld). Artinya, seseorang hanya dapat dimintai pertanggungjawaban pidana atas kejahatan siber apabila perbuatannya memenuhi rumusan delik yang ditentukan undang-undang dan dilakukan dengan unsur kesalahan, baik berupa kesengajaan (dolus) maupun kealpaan (culpa). Namun, penerapan asas-asas tersebut dalam konteks cybercrime sering kali menimbulkan perdebatan, terutama dalam menilai unsur kesengajaan pada perbuatan yang dilakukan melalui sistem otomatis atau platform digital.

Ruang Lingkup Kejahatan Siber dalam Undang-Undang Informasi dan Transaksi Elektronik

Ruang lingkup kejahatan siber dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) tidak dapat dipahami secara sempit hanya sebagai kejahatan yang menyerang teknologi atau sistem komputer semata. Sebaliknya, UU ITE membangun suatu rezim hukum pidana yang memposisikan teknologi informasi sebagai medium utama terjadinya kejahatan, sekaligus sebagai objek hukum yang dilindungi. Oleh karena itu, ruang lingkup cybercrime dalam UU ITE bersifat multidimensional, mencakup dimensi teknologis, sosial, ekonomi, dan hukum pidana.

Secara filosofis, pembentukan UU ITE dilandasi oleh kebutuhan untuk memberikan kepastian hukum dalam pemanfaatan teknologi informasi, sekaligus melindungi masyarakat dari dampak negatif penyalahgunaan teknologi tersebut. Kejahatan siber dipandang sebagai ancaman terhadap kepentingan hukum yang bersifat non-fisik namun berdampak nyata, seperti kehormatan, rasa aman, kepercayaan publik, serta stabilitas transaksi elektronik. Dengan demikian, ruang lingkup cybercrime dalam UU ITE diarahkan tidak hanya pada perlindungan sistem elektronik, tetapi juga pada perlindungan nilai-nilai fundamental dalam kehidupan bermasyarakat.Dari perspektif normatif, ruang lingkup kejahatan siber dalam UU ITE tercermin dalam ketentuan Pasal 27 sampai dengan Pasal 37, yang selanjutnya dipertegas melalui ketentuan sanksi pidana dalam Pasal 45 sampai dengan Pasal 52. Ketentuan-ketentuan tersebut membentuk suatu konstruksi hukum pidana khusus (lex specialis) yang melengkapi bahkan dalam batas tertentu menyimpangi hukum pidana umum sebagaimana diatur dalam KUHP. Hal ini menunjukkan bahwa pembentuk undang-undang menyadari adanya karakteristik khusus kejahatan siber yang tidak sepenuhnya dapat diakomodasi oleh hukum pidana konvensional.

Ruang lingkup kejahatan siber dalam UU ITE dapat dianalisis dari tiga aspek utama, yaitu aspek perbuatan (actus reus), aspek sarana, dan aspek kepentingan hukum yang dilindungi. Dari aspek perbuatan, UU ITE mengkriminalisasi tindakan-tindakan tertentu seperti mendistribusikan, mentransmisikan, membuat dapat diaksesnya, mengakses tanpa hak, serta melakukan intervensi terhadap sistem dan data elektronik. Rumusan perbuatan ini bersifat khas dan tidak ditemukan secara eksplisit dalam KUHP, sehingga menegaskan kekhususan delik-delik UU ITE. Dari aspek sarana, ruang lingkup cybercrime dalam UU ITE secara tegas mensyaratkan adanya penggunaan sistem elektronik atau jaringan teknologi informasi. Sistem elektronik dalam UU ITE tidak hanya dipahami sebagai perangkat keras (hardware), tetapi juga mencakup perangkat lunak (software), jaringan, serta prosedur elektronik yang saling terintegrasi. Konsekuensinya, setiap perbuatan melawan hukum yang dilakukan melalui media tersebut berpotensi masuk dalam ruang lingkup kejahatan siber, sepanjang memenuhi unsur delik yang ditentukan undang-undang).

METODE PENELITIAN

Jenis Penelitian

Penelitian ini merupakan penelitian hukum normatif (normative legal research), yaitu penelitian yang dilakukan dengan menelaah norma-norma hukum positif yang berlaku, asas-asas hukum, doktrin, serta putusan pengadilan yang berkaitan dengan soalan ini. Penelitian hukum normatif dipilih karena permasalahan utama yang dikaji cybercrime

Pendekatan Penelitian

1) Pendekatan yang digunakan dalam penelitian ini adalah:
2) Pendekatan Perundang-undangan (statute approach), dengan menelaah berbagai peraturan perundang-undangan yang relevan, seperti UUITE, Kitab Undang-Undang Hukum pidana, peraturan terkait pencatatan perkawinan.
3) Pendekatan Konseptual (conceptual approach), yaitu menggunakan pandangan para ahli hukum dan doktrin yang berkembang untuk memahami konsep judul ini.
4) Pendekatan Kasus (case approach), yaitu dengan menelaah putusan pengadilan.

Metode Pengumpulan Bahan Hukum

Dalam melakukan pengumpulan bahan hukum dilakukan dengan penelusuran dokumen baik secara on-line dan/atau off-line. Penelusuran secara on-line dilakukan dengan membuka (browsing) situs internet, berkomunikasi melalui e-mail dan/atau melalui pesan singkat dan/atau melalui jaringan telekomunikasi berupa telepone. Penelusuran secara off-line dilakukan dengan berkunjung untuk membaca dan membuat catatan dari beberapa perpustakaan, toko buku, dan meminjam literatur dengan rekan-rekan. Dengan kata lain,pengumpulan bahan hukum dalam penelitianini menggunakan metode studi dokumen atau “literature study”. Data yang diperlukan sudah tertulis atau diolah oleh orang lain atau suatu lembaga.

Analisis Bahan Hukum

Analisis bahan hukum dilakukan untuk menjawab masalah penelitian yang telah dirumuskan. Analisis bahan hukum yang telah dikumpulkan dilakukan dengan cara interpretasi dan content analysis. Untuk bahan hukum primer, analisis dilakukan dengan cara interpretasi (penafsiran). Penafsiran yang digunakan dalam penelitian, yaitu penafsiran gramatikal (taatkundige interpetatie) dan penafsiran otentik. Penafsiran gramatikal, yaitu penafsiran yang dilakukan terhadap peristilahan atau kata-kata, tata kalimat di dalam suatu konteks bahasa yang digunakan pembuat Undang-Undang dalam merumuskan peraturan Perundang-Undangan tertentu. Penafsiran otentik adalah penafsiran terhadap kata, istilah atau pengertian di dalam peraturan Perundang-Undangan yang telah ditetapkan sebelumnya oleh pembuat Undang-Undang sendiri.

HASIL DAN PEMBAHASAN

Pengaturan mengenai pertanggungjawaban pidana pelaku kejahatan siber dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan respons hukum terhadap pesatnya perkembangan teknologi informasi dan komunikasi yang memunculkan bentuk-bentuk kejahatan baru di ruang siber. Kejahatan siber memiliki karakteristik khusus, antara lain dilakukan melalui sistem elektronik, bersifat lintas batas negara, serta menggunakan data dan informasi digital sebagai sarana maupun objek kejahatan. Kondisi ini menuntut adanya pengaturan hukum pidana yang bersifat khusus (lex specialis) guna menjamin kepastian hukum dan perlindungan terhadap kepentingan masyarakat di era digital. UU ITE tidak memberikan definisi eksplisit mengenai cybercrime, namun secara substansial mengatur berbagai perbuatan yang dapat dikualifikasikan sebagai tindak pidana di bidang teknologi informasi. Perbuatan tersebut meliputi penyalahgunaan informasi elektronik, pelanggaran terhadap sistem elektronik, serta tindakan manipulatif terhadap data elektronik yang dapat menimbulkan kerugian bagi individu, masyarakat, maupun negara. Konsep kejahatan siber dalam UU ITE dipahami melalui perumusan delik-delik pidana yang tersebar dalam berbagai pasal, khususnya Pasal 27 sampai dengan Pasal 35. Pertanggungjawaban pidana dalam UU ITE didasarkan pada pengakuan terhadap subjek hukum yang luas. Subjek hukum tidak hanya mencakup orang perseorangan, tetapi juga badan hukum atau korporasi. Hal ini ditegaskan dalam ketentuan Pasal 1 angka 21 UU ITE yang menyatakan bahwa “orang” adalah orang perseorangan atau badan hukum. Konsepsi ini menunjukkan bahwa pembentuk undang-undang telah mengantisipasi

kemungkinan kejahatan siber dilakukan secara terorganisir oleh entitas bisnis atau korporasi yang memanfaatkan teknologi informasi dalam menjalankan kegiatannya.

Dalam konteks hukum pidana, pertanggungjawaban pidana pelaku cybercrime tetap berlandaskan pada asas kesalahan, yakni tidak ada pidana tanpa kesalahan (geen straf zonder schuld). Oleh karena itu, untuk dapat dimintakan pertanggungjawaban pidana, pelaku harus terbukti melakukan perbuatan yang dilarang dengan kesengajaan atau setidak-tidaknya kealpaan. UU ITE secara konsisten mencantumkan unsur "dengan sengaja dan tanpa hak atau melawan hukum" dalam rumusan delik pidananya. Unsur ini menunjukkan bahwa kesengajaan merupakan elemen utama dalam menentukan dapat atau tidaknya pelaku dimintai pertanggungjawaban pidana atas perbuatannya di ruang siber. Lebih lanjut, UU ITE mengatur berbagai bentuk tindak pidana siber yang dapat menimbulkan pertanggungjawaban pidana. Tindak pidana tersebut antara lain perbuatan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang bermuatan melanggar hukum, seperti muatan kesusilaan, perjudian, penghinaan, pencemaran nama baik, pemerasan, dan ancaman. Selain itu, UU ITE juga mengatur tindak pidana yang berkaitan dengan pelanggaran terhadap sistem elektronik, seperti akses ilegal, penyadapan tanpa hak, serta perusakan atau pengubahan data elektronik. Seluruh perbuatan tersebut dipandang sebagai pelanggaran serius karena dapat mengganggu keamanan, keandalan, dan kepercayaan terhadap sistem elektronik.

Pengaturan pertanggungjawaban pidana dalam UU ITE juga mencakup kemungkinan pemidanaan terhadap korporasi. Dalam hal tindak pidana siber dilakukan oleh atau atas nama korporasi, maka pertanggungjawaban pidana dapat dibebankan kepada korporasi dan/atau pengurusnya. Ketentuan ini tercermin dalam Pasal 52 UU ITE yang memberikan dasar hukum bagi penjatuhan pidana denda dengan pemberatan tertentu terhadap korporasi. Pengaturan ini sejalan dengan perkembangan hukum pidana modern yang mengakui korporasi sebagai subjek hukum pidana, terutama dalam konteks kejahatan yang bersifat kompleks dan berbasis teknologi. Aspek lain yang tidak kalah penting dalam pertanggungjawaban pidana cybercrime adalah pengaturan mengenai yurisdiksi. Mengingat kejahatan siber bersifat lintas batas dan tidak mengenal wilayah teritorial secara fisik, UU ITE memperluas jangkauan berlakunya hukum pidana nasional. Pasal 2 UU ITE menegaskan bahwa undang-undang ini berlaku bagi setiap orang, baik yang berada di dalam maupun di luar wilayah hukum Indonesia, sepanjang perbuatannya memiliki akibat hukum di Indonesia. Ketentuan ini memberikan dasar bagi negara untuk menuntut pelaku kejahatan siber yang merugikan kepentingan hukum nasional, meskipun dilakukan dari luar wilayah Indonesia. Maka dapat dilihat, secara normatif UU ITE telah mengatur pertanggungjawaban pidana pelaku kejahatan siber secara relatif komprehensif, mencakup aspek subjek hukum, asas kesalahan, jenis perbuatan pidana, sanksi, serta yurisdiksi. Meskipun demikian, tantangan utama dalam penerapannya terletak pada pembuktian unsur-unsur pidana yang berbasis teknologi serta perlunya penafsiran hukum yang cermat agar penegakan hukum di ruang siber tetap menjunjung tinggi asas keadilan dan kepastian hukum.

KESIMPULAN DAN SARAN

Berdasarkan hasil kajian dan pembahasan mengenai pertanggungjawaban pidana pelaku kejahatan siber (cybercrime) menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dapat disimpulkan bahwa pembentukan UU ITE merupakan langkah hukum strategis negara dalam merespons perkembangan teknologi informasi dan komunikasi yang melahirkan bentuk-bentuk kejahatan baru di ruang siber. UU ITE berfungsi sebagai hukum pidana khusus (lex specialis) yang melengkapi ketentuan hukum pidana umum dalam Kitab Undang-Undang Hukum Pidana (KUHP) guna memberikan kepastian dan perlindungan hukum di era digital.Pengaturan pertanggungjawaban pidana dalam UU ITE pada prinsipnya tetap berlandaskan asas fundamental hukum pidana, yaitu asas kesalahan (geen straf zonder schuld). Seseorang hanya dapat dimintai pertanggungjawaban pidana apabila terbukti secara sah dan meyakinkan telah melakukan perbuatan yang dilarang dengan kesengajaan atau kealpaan, serta tanpa hak atau melawan hukum. Unsur kesalahan tersebut tercermin secara konsisten dalam perumusan delik-delik pidana siber yang diatur dalam Pasal 27 sampai dengan Pasal 35 UU ITE.

Selain itu, UU ITE telah memperluas cakupan subjek hukum yang dapat dimintai pertanggungjawaban pidana, tidak hanya terbatas pada orang perseorangan, tetapi juga badan hukum atau korporasi. Pengakuan terhadap korporasi sebagai subjek hukum pidana menunjukkan adanya penyesuaian hukum pidana terhadap realitas kejahatan siber yang sering kali dilakukan secara terorganisir dan melibatkan entitas bisnis berbasis teknologi. Dengan demikian, pertanggungjawaban pidana dalam UU ITE mencerminkan perkembangan hukum pidana modern yang adaptif terhadap dinamika teknologi informasi.Namun demikian, hasil kajian juga menunjukkan bahwa meskipun secara

normatif UU ITE telah mengatur pertanggungjawaban pidana pelaku kejahatan siber secara relatif komprehensif, penerapannya dalam praktik penegakan hukum masih menghadapi berbagai kendala. Kendala tersebut meliputi kesulitan pembuktian berbasis bukti elektronik, keterbatasan kapasitas aparat penegak hukum, karakter kejahatan siber yang bersifat lintas batas negara, serta potensi multitafsir dalam beberapa ketentuan pidana. Kondisi ini berdampak pada belum optimalnya penegakan hukum pidana terhadap pelaku cybercrime dan berpotensi menimbulkan ketidakpastian hukum.Dengan demikian, dapat disimpulkan bahwa pertanggungjawaban pidana pelaku kejahatan siber menurut UU ITE telah memiliki dasar hukum yang kuat, namun masih memerlukan penguatan dari aspek implementasi agar tujuan hukum pidana, yaitu kepastian hukum, keadilan, dan kemanfaatan, dapat tercapai secara seimbang di ruang siber.

DAFTAR PUSTAKA

Arrasjid, Chainur. 2004. Dasar-Dasar Ilmu Hukum. Jakarta: Sinar Grafika.

Arief, Barda Nawawi. 2006. Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia. Jakarta: RajaGrafindo Persada.

———. 2007. Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana.

———. 2016. Bunga Rampai Kebijakan Hukum Pidana. Jakarta: Kencana.

———. 2018. Kebijakan Formulasi Hukum Pidana. Jakarta: Kencana.

Ashworth, Andrew. 2010. Sentencing and Criminal Justice. 5th ed. Cambridge: Cambridge University Press.

Atmasasmita, Romli. 2011. Sistem Peradilan Pidana Kontemporer. Jakarta: Kencana.

———. 2017. Rekonstruksi Asas Tiada Pidana Tanpa Kesalahan. Jakarta: Gramedia Pustaka Utama.

Bassiouni, M. Cherif. 2008. International Criminal Law: Volume II: Multilateral and Bilateral Enforcement Mechanisms. 3rd ed. Leiden: Martinus Nijhoff Publishers.

Beccaria, Cesare. 1963. On Crimes and Punishments. Translated by Henry Paolucci. Indianapolis: Bobbs-Merrill.

Brenner, Susan W. 2010. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger.

Brownlie, Ian. 2008. Principles of Public International Law. 7th ed. Oxford: Oxford University Press.

Chazawi, Adami. 2011. Pelajaran Hukum Pidana Bagian I. Jakarta: RajaGrafindo Persada.

Clough, Jonathan. 2015. Principles of Cybercrime. 2nd ed. Cambridge: Cambridge University Press.

Council of Europe. 2001. Budapest Convention on Cybercrime. Strasbourg: Council of Europe.

Djafar, Wahyudi dan Donny B.U. 2017. Problematika Implementasi Undang-Undang Informasi dan Transaksi Elektronik. Jakarta: ELSAM.

Eddyono, Supriyadi Widodo. 2017. Hukum Pidana dan Kebebasan Berekspresi. Jakarta: ELSAM.

Feuerbach, Paul Johann Anselm von. 1847. Lehrbuch des gemeinen in Deutschland gültigen peinlichen Rechts. 14th ed. Giessen: Georg Friedrich Heyer.

Friedman, Lawrence M. 2000. Law and Society: An Introduction. New Jersey: Prentice Hall.

Goldsmith, Jack L. dan Tim Wu. 2006. Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.

Hall, Jerome. 1960. General Principles of Criminal Law. 2nd ed. Indianapolis: Bobbs-Merrill.

Hamzah, Andi. 2008. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

———. 2010. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

———. 2019. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

Hart, H.L.A. 1968. Punishment and Responsibility: Essays in the Philosophy of Law. Oxford: Clarendon Press.

Hiariej, Eddy O.S. 2014. Prinsip-Prinsip Hukum Pidana. Yogyakarta: Cahaya Atma Pustaka.

Hingorani, R.C. 1984. Modern International Law. 2nd ed. New Delhi: Oceana Publications.

Huda, Chairul. 2006. Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan. Jakarta: Kencana.

Ibrahim, Johnny. 2006. Teori dan Metodologi Penelitian Hukum Normatif. Malang: Bayumedia Publishing.

Kanter, E.Y. dan S.R. Sianturi. 2012. Asas-Asas Hukum Pidana di Indonesia dan Penerapannya. Jakarta: Storia Grafika.

Kartanegara, Satochid. 2002. Hukum Pidana Kumpulan Kuliah Bagian Satu. Jakarta: Balai Lektur Mahasiswa.

Kshetri, Nir. 2010. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin: Springer.

LaFave, Wayne R. 2010. Criminal Law. 5th ed. St. Paul: West Publishing.

Lamintang, P.A.F. 1997. Dasar-Dasar Hukum Pidana Indonesia. Bandung: Citra Aditya Bakti.
———. 2013. Dasar-Dasar Hukum Pidana Indonesia. Bandung: Citra Aditya Bakti.
Lessig, Lawrence. 2006. Code: And Other Laws of Cyberspace. Version 2.0. New York: Basic Books.
Makarim, Edmon. 2005. Pengantar Hukum Telematika: Suatu Kompilasi Kajian. Jakarta: RajaGrafindo Persada.
———. 2014. Pengantar Hukum Telematika. Jakarta: RajaGrafindo Persada.
Mansur, Dikdik M. Arief dan Elisatris Gultom. 2005. Cyber Law: Aspek Hukum Teknologi Informasi. Bandung: Refika Aditama.
Marpaung, Leden. 2005. Asas-Teori-Praktik Hukum Pidana. Jakarta: Sinar Grafika.
———. 2009. Asas-Teori-Praktik Hukum Pidana. Jakarta: Sinar Grafika.
Marzuki, Peter Mahmud. 2011. Penelitian Hukum. Jakarta: Kencana Prenada Media Group.
Moeljatno. 2008. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
———. 2015. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
Morris, Norval dan Michael Tonry. 1990. Between Prison and Probation. New York: Oxford University Press.
Muladi dan Barda Nawawi Arief. 2005. Teori-Teori dan Kebijakan Pidana. Bandung: Alumni.
Muladi dan Dwidja Priyatno. 2010. Pertanggungjawaban Pidana Korporasi. Jakarta: Kencana Prenada Media Group.
Packer, Herbert L. 1968. The Limits of the Criminal Sanction. Stanford: Stanford University Press.
Prodjodikoro, Wirjono. 2003. Asas-Asas Hukum Pidana di Indonesia. Bandung: Refika Aditama.
Purwoleksono, Didik Endro. 2019. Hukum Pidana Siber (Cybercrime). Surabaya: Airlangga University Press.
Rahardjo, Satjipto. 2009. Hukum dalam Perspektif Sosial. Yogyakarta: Genta Publishing.
Rawls, John. 1971. A Theory of Justice. Cambridge: Harvard University Press.
Remmelink, Jan. 2003. Hukum Pidana: Komentar atas Pasal-Pasal Terpenting KUHP. Jakarta: Gramedia Pustaka Utama.
Saleh, Roeslan. 1983. Perbuatan Pidana dan Pertanggungjawaban Pidana. Jakarta: Aksara Baru.
———. 1987. Stelsel Pidana Indonesia. Jakarta: Aksara Baru.
Sholehuddin, M. 2003. Sistem Sanksi dalam Hukum Pidana. Jakarta: RajaGrafindo Persada.
Sianturi, S.R. 1996. Asas-Asas Hukum Pidana di Indonesia. Jakarta: Alumni Ahaem-Petehaem.
Singer, Richard G. dan John Q. La Fond. 2010. Criminal Law. 5th ed. New York: Wolters Kluwer.
Sitompul, Josua. 2012. Cyberspace, Cybercrimes, Cyberlaw. Jakarta: Tatanusa.
Soekanto, Soerjono. 1990. Kriminologi: Suatu Pengantar. Jakarta: UI Press.
Soekanto, Soerjono dan Sri Mamudji. 2001. Penelitian Hukum Normatif. Jakarta: RajaGrafindo Persada.
Sudarto. 1990. Hukum Pidana I. Semarang: Yayasan Sudarto.
———. 2007. Hukum dan Hukum Pidana. Bandung: Alumni.
Suhariyanto, Budi. 2013. Tindak Pidana Teknologi Informasi (Cybercrime). Jakarta: Rajawali Pers.

Suseno, Sigid. 2011. “Kejahatan Dunia Maya dan Permasalahannya.” Jurnal Hukum dan Pembangunan 41(3): 322–336.
———. 2012. Yurisdiksi Tindak Pidana Siber. Bandung: Refika Aditama.
Tonry, Michael. 1996. Sentencing Matters. New York: Oxford University Press.
United Nations Office on Drugs and Crime (UNODC). 2013. Comprehensive Study on Cybercrime. New York: United Nations.
Wall, David S. 2007. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.
Williams, Glanville. 1961. Criminal Law: The General Part. 2nd ed. London: Stevens & Sons