



Analisis Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Terorisme Berbasis Informasi dan Transaksi Teknologi

Hibni Abdillah¹, Nafidz Revaldi Putrawan²

^{1,2}Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Bandar Lampung, Indonesia
E-mail: hibniabdillah48@gmail.com¹, minakrevaldi2015@gmail.com²

Article Info

Article history:

Received Agust 05, 2025

Revised Agust 12, 2025

Accepted Agust 16, 2025

Keywords:

Criminal Liability, Terrorism
Crime, Information
Technology, Criminal Law,
ITE.

ABSTRACT

Cyber-based terrorism is a modern crime utilizing digital platforms to spread extremist ideologies and coordinate acts of violence. This study analyzes criminal liability for perpetrators of digital terrorism through a legal theory framework and applicable regulations. Using a qualitative approach and library research method, the study examines relevant legal concepts, statutes, and court decisions. The findings reveal that major obstacles lie in evidentiary challenges and regulatory gaps. It concludes that legal reform and capacity-building for law enforcement are essential to ensure effective and fair prosecution of terrorism committed via information technology.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Article Info

Article history:

Received Agust 05, 2025

Revised Agust 12, 2025

Accepted Agust 16, 2025

Kata Kunci:

Pertanggungjawaban Pidana,
Tindak Pidana Terorisme,
Teknologi Informasi, Hukum
Pidana, ITE.

ABSTRAK

Tindak pidana terorisme berbasis teknologi informasi merupakan bentuk kejahatan modern yang memanfaatkan dunia digital untuk menyebarkan ideologi ekstrem dan merancang aksi kekerasan. Studi ini bertujuan menganalisis pertanggungjawaban pidana terhadap pelaku terorisme digital berdasarkan tinjauan teori hukum pidana dan kerangka peraturan yang berlaku. Melalui pendekatan kualitatif dengan metode studi kepustakaan, penelitian ini mengkaji konsep, peraturan, dan putusan hukum yang relevan. Hasil pembahasan menunjukkan bahwa kendala utama terdapat pada aspek pembuktian dan ketidaksesuaian regulasi. Kesimpulannya, perlu pembaruan hukum dan peningkatan kapasitas penegak hukum dalam menangani terorisme berbasis ITE secara efektif dan adil.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Hibni Abdillah

Program Studi Ilmu Hukum, Fakultas Hukum Universitas Bandar Lampung

E-mail: hibniabdillah48@gmail.com



Pendahuluan

Dalam beberapa tahun terakhir, kemajuan teknologi informasi dan komunikasi telah merevolusi pola interaksi, komunikasi, dan pertukaran informasi antarindividu. Namun, di balik berbagai manfaat yang ditawarkan, perkembangan ini juga menciptakan celah bagi munculnya berbagai jenis kejahatan, termasuk tindak kejahatan seksual yang dilakukan melalui media digital.¹

Perkembangan teknologi informasi yang pesat di era digital telah membuka berbagai kemudahan dalam komunikasi dan akses informasi. Namun, di sisi lain, kemajuan ini juga dimanfaatkan oleh kelompok-kelompok radikal untuk menyebarkan ideologi kekerasan dan menjalankan aktivitas terorisme secara tersembunyi dan masif. Fenomena tindak pidana terorisme berbasis informasi dan transaksi elektronik (ITE) telah menjadi tantangan baru bagi sistem hukum pidana di Indonesia. Pelaku tidak lagi hanya melakukan tindakan kekerasan secara fisik, tetapi juga menggunakan platform digital untuk merekrut, mendanai, menyebarkan propaganda, dan bahkan merencanakan aksi teror.²

Menurut laporan Badan Nasional Penanggulangan Terorisme (BNPT), pola rekrutmen dan penyebaran doktrin radikalisme melalui media sosial meningkat tajam dalam satu dekade terakhir. Tindak pidana ini melibatkan penggunaan sarana digital untuk tujuan yang bertentangan dengan keamanan negara dan ketertiban umum. Dalam konteks ini, pelaku terorisme tidak hanya melanggar ketentuan Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, tetapi juga dapat dijerat melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Hal ini menimbulkan pertanyaan hukum mengenai bentuk pertanggungjawaban pidana yang dapat dikenakan terhadap pelaku dalam ranah kejahatan siber yang berkorelasi dengan aksi teror.

Dari perspektif teori hukum pidana, pertanggungjawaban pidana menekankan pada unsur kesalahan (*mens rea*) dan perbuatan melawan hukum (*actus reus*) yang dilakukan secara sadar oleh pelaku. Namun, dalam kasus terorisme berbasis ITE, sering kali ditemukan kompleksitas seperti penggunaan akun palsu, jaringan terdesentralisasi, dan teknik penyamaran digital (enkripsi atau *dark web*), yang menyulitkan penegak hukum dalam membuktikan intensi dan keterlibatan langsung. Oleh karena itu, dibutuhkan pendekatan analitis terhadap konsep pertanggungjawaban pidana yang adaptif terhadap kejahatan modern berbasis teknologi.

Sistem peradilan pidana merupakan suatu mekanisme terpadu dalam penegakan hukum pidana, yang melibatkan kepolisian, kejaksaan, pengadilan, dan lembaga pemasyarakatan sebagai subsistem yang saling berhubungan dan berinteraksi. Tujuan utama dari sistem ini adalah menciptakan keadilan, kepastian hukum, serta kemanfaatan hukum melalui pendekatan normatif, administratif, dan sosial yang menyeluruh.³ Urgensi penelitian ini diperkuat oleh kenyataan bahwa hingga kini masih terdapat kekosongan norma dan tumpang tindih kewenangan dalam penanganan tindak pidana terorisme digital. Penegakan

¹ Abdullah Husein Al Aziz and Zainudin Hasan, 'Pertanggungjawaban Pidana Pelaku Tindak Pidana Pengancaman Dengan Revenge Porn Dalam Era Digital Di Kota Bandar Lampung', *Jurnal Hukum, Politik Dan Ilmu Sosial*, 3.4 (2024), pp. 341–55, doi:10.55606/jhpis.v3i4.4476.

² Muhammad Arkhan Maulana Bastian, Rudy Sutanto, and Raden Ruli Basuni, 'Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Dalam Pencegahan Cyberterrorism', *Jurnal Hukum Mimbar Justitia*, 10.2 (2025), p. 430, doi:10.35194/jhmj.v10i2.4997.

³ Zainudin Hasan. 2025. "Sistem Peradilan Pidana Penjara", CV. Alinea Edumedia, Cilacap, hlm. 5.



hukum cenderung reaktif dan belum sepenuhnya berbasis pada penegakan preventif dan restorative, padahal pendekatan tersebut lebih relevan dalam menangani ancaman terorisme yang bersifat transnasional dan lintas batas digital. Di samping itu, aparat penegak hukum juga menghadapi tantangan dalam menyeimbangkan antara perlindungan hak asasi manusia dan penindakan terhadap pelaku teror yang memanfaatkan ruang digital.

Dengan demikian, penelitian ini penting untuk menganalisis bagaimana bentuk pertanggungjawaban pidana yang dapat diterapkan terhadap pelaku tindak pidana terorisme berbasis ITE, serta mengkaji relevansi dan efektivitas perangkat hukum yang ada. Kajian ini diharapkan dapat memberikan kontribusi teoritis maupun praktis dalam pengembangan sistem hukum pidana nasional yang responsif terhadap perkembangan modus kejahatan era digital. Penelitian ini juga menjadi upaya kritis dalam memperkuat kebijakan hukum yang tidak hanya bersifat represif, tetapi juga berorientasi pada keadilan substantif dan perlindungan masyarakat secara komprehensif dari ancaman terorisme digital.

Kajian Pustaka

A. Pengertian Tindak Pidana Terorisme Berbasis ITE

Tindak pidana terorisme berbasis ITE merupakan bentuk kejahatan yang menggabungkan unsur kekerasan ekstrem dengan pemanfaatan teknologi informasi sebagai sarana atau objek kejahatan. Menurut Undang-Undang Nomor 5 Tahun 2018, terorisme didefinisikan sebagai perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, dengan motif ideologi, politik, atau keamanan. Ketika aktivitas ini dilakukan melalui media digital, seperti penyebaran konten radikal, perekrutan online, dan pendanaan virtual, maka masuk dalam kategori kejahatan siber dengan muatan terorisme.⁴

Kemajuan pesat dalam bidang Teknologi Informasi dan Komunikasi turut memunculkan berbagai bentuk penyalahgunaan yang mengkhawatirkan. Salah satu dampak negatif yang mencuat adalah meningkatnya tindak kejahatan di ranah digital, yang kini lebih dikenal dengan istilah *cybercrime*.⁵ Pemanfaatan teknologi dalam aksi teror telah membuka dimensi baru dalam penanganan kejahatan, karena pelaku tidak selalu hadir secara fisik di lokasi kejadian. Sebaliknya, mereka dapat mengendalikan tindakan teror dari jarak jauh melalui jaringan internet. Hal ini membuat aparat penegak hukum memerlukan pemahaman yang mendalam terhadap cara kerja sistem digital dan hukum siber, sehingga penindakan tidak hanya berdasarkan akibat nyata, tetapi juga berdasarkan aktivitas elektronik yang melanggar hukum dan berdampak terhadap keamanan nasional.

B. Teori Pertanggungjawaban Pidana

Di era digital saat ini, informasi telah menjadi kebutuhan utama bagi masyarakat. Dengan adanya kemudahan akses terhadap media dan jaringan internet, publik dapat dengan cepat memperoleh sekaligus mendistribusikan informasi melalui berbagai platform digital.⁶

⁴ Cyber-terrorism Dari Sudut and Pandang Hukum, 'Cyber-Terrorism Dari Sudut Pandang Hukum Pidana Indonesia', pp. 1-13.

⁵ Zainudin Hasan and others, 'Peranan Cyber Law Dalam Penanganan Tindak Pidana Di Indonesia', *Jurnal Komunikasi*, 2.5 (2024), pp. 337-45.

⁶ Muhammad Iqbal, Heru Juli Ardie, and Zainudin Hasan, 'Analisis Hukum Dalam Melacak Jejak Digital Dan Memahami Tindak Pidana Pencucian Uang Dalam Era Teknologi', *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*, 5 (2024), pp. 286-98, doi:10.24252/iqtishaduna.vi.43802.



Pertanggungjawaban pidana dalam ilmu hukum pidana merujuk pada mekanisme untuk menetapkan kesalahan pelaku yang telah melakukan perbuatan yang melawan hukum. Menurut teori klasik, pertanggungjawaban pidana memerlukan adanya kesalahan berupa kesengajaan (*dolus*) atau kelalaian (*culpa*) yang dilakukan oleh pelaku yang mampu mempertanggungjawabkan perbuatannya secara hukum. Unsur ini menjadi dasar untuk menjatuhkan sanksi pidana sebagai bentuk pembalasan dan perlindungan masyarakat.

Bantuan hukum merupakan hak konstitusional setiap warga negara untuk mendapatkan perlakuan yang adil di hadapan hukum tanpa diskriminasi. Hal ini menjadi bentuk implementasi dari prinsip negara hukum yang menjamin akses terhadap keadilan, khususnya bagi masyarakat miskin dan kelompok rentan yang tidak memiliki sumber daya untuk menyewa penasihat hukum secara mandiri.⁷

Dalam konteks kejahatan berbasis ITE, penerapan teori pertanggungjawaban pidana menghadapi tantangan tersendiri. Banyak kasus menunjukkan bahwa pelaku menggunakan identitas samaran atau jaringan virtual yang sulit dilacak. Oleh karena itu, pendekatan hukum pidana harus disesuaikan dengan perkembangan teknologi, termasuk dengan memperluas konsep perbuatan pidana (*actus reus*) dan niat jahat (*mens rea*) agar dapat mencakup tindakan-tindakan yang terjadi di ruang digital, sekaligus tetap menjamin keadilan dan kepastian hukum.

C. Landasan Hukum Penanggulangan Terorisme Digital

Penegakan hukum meliputi serangkaian tahapan mulai dari penerapan norma hukum, pengawasan pelaksanaannya, penindakan terhadap pelanggaran, upaya pemulihan atas pelanggaran yang terjadi, hingga menjamin terselenggaranya proses yang transparan dan akuntabel.⁸ Penanggulangan tindak pidana terorisme yang menggunakan sarana teknologi informasi di Indonesia didasarkan pada dua kerangka hukum utama, yaitu Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Kedua regulasi ini saling melengkapi, di mana UU Terorisme mengatur substansi ancaman dan pelaku, sementara UU ITE menekankan aspek medium dan proses penyebaran informasi yang digunakan dalam tindak pidana tersebut.

Namun, sinkronisasi antar regulasi ini masih menghadapi berbagai tantangan normatif dan implementatif. Salah satu isu utama adalah belum adanya ketentuan yang secara eksplisit merumuskan bentuk-bentuk tindak pidana terorisme digital, sehingga membuka ruang interpretasi yang luas dalam proses penegakan hukum. Oleh karena itu, analisis mendalam terhadap efektivitas instrumen hukum tersebut menjadi penting untuk memastikan bahwa sistem peradilan pidana mampu menjawab tantangan kejahatan terorisme di era siber secara komprehensif dan akuntabel.⁹

⁷ Zainudin Hasan. 2025. "*Hukum Pidana*", CV. Alinea Edumedia, Cilacap, hlm. 46-50.

⁸ Zainudin Hasan. 2025. "*Penegak Hukum Dan Penegakan Hukum Di Indonesia*", Universitas Bandar Lampung (UBL) Press, Bandar Lampung, hlm. 11.

⁹ Yusril Iman Wahyudi, Nining Haslinda Zainal, and Ade Ferry Afrisal, 'Indeks Kepuasan Masyarakat Terhadap Pelayanan Perizinan Berbasis Aplikasi OSS Di Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Kabupaten Pinrang', *Publician: Journal of Public Service, Public Policy, and Administrastion*, 3.1 (2024), pp. 44-50, doi:10.56326/jp.v3i1.4135.



Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kepustakaan (library research). Pendekatan ini dipilih karena fokus utama kajian adalah menganalisis konsep, teori hukum, serta peraturan perundang-undangan yang berkaitan dengan pertanggungjawaban pidana terhadap pelaku tindak pidana terorisme berbasis ITE. Metode ini memungkinkan peneliti untuk menggali data secara mendalam melalui interpretasi teks hukum, doktrin, dan hasil penelitian terdahulu yang relevan, guna membangun argumentasi hukum yang sistematis dan logis.¹⁰

Sumber data dalam penelitian ini terdiri dari data sekunder, yaitu bahan hukum primer seperti Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, serta bahan hukum sekunder seperti buku-buku hukum pidana, jurnal ilmiah, artikel hukum, dan pendapat para ahli. Teknik pengumpulan data dilakukan melalui penelusuran sistematis terhadap dokumen, regulasi, dan literatur ilmiah dari perpustakaan, jurnal online bereputasi, dan arsip hukum yang relevan.

Analisis data dilakukan secara deskriptif-analitis, dengan menafsirkan isi dokumen hukum berdasarkan pendekatan normatif dan teoritik. Tujuannya adalah untuk mengkaji sejauh mana aturan yang ada mampu menampung bentuk pertanggungjawaban pidana terhadap pelaku terorisme digital, serta untuk mengidentifikasi celah hukum dan memberikan saran perbaikan. Dengan metode ini, penelitian diharapkan dapat memberikan kontribusi konseptual dan praktis dalam penguatan sistem hukum pidana nasional yang adaptif terhadap dinamika kejahatan berbasis teknologi informasi.

Hasil dan Pembahasan

A. Pola dan Modus Operandi Terorisme Berbasis ITE di Indonesia

Perkembangan teknologi digital telah mengubah cara kerja kelompok teror. Jika sebelumnya aksi terorisme dilakukan secara fisik dan langsung, saat ini pelaku mulai menggunakan media sosial, forum daring, dan platform komunikasi terenkripsi untuk menyebarkan propaganda dan merekrut anggota. Modus ini memanfaatkan anonimitas dunia maya untuk menghindari pelacakan dan hukum formal.¹¹

Selain hambatan teknis dalam pembuktian dan identifikasi pelaku, implementasi pertanggungjawaban pidana terhadap pelaku terorisme digital juga menghadapi tantangan yuridis terkait kepastian hukum. UU No. 5 Tahun 2018 belum secara spesifik menyebutkan bentuk-bentuk kejahatan yang dilakukan melalui internet sebagai bagian dari tindak pidana terorisme. Akibatnya, aparat penegak hukum sering kali harus melakukan konstruksi hukum berdasarkan interpretasi luas, yang dalam praktiknya dapat menimbulkan multitafsir dan potensi pelanggaran prinsip legalitas dalam hukum pidana.

Lebih lanjut, tidak adanya klasifikasi khusus mengenai "cyber terrorism" dalam hukum positif Indonesia membuat pengenaan sanksi pidana terhadap pelaku menjadi kurang proporsional. Sebagian kasus justru dikenakan pasal dalam UU ITE yang cenderung lebih

¹⁰ Frank Jacob, 'Cyber Terrorism', *Encyclopedia of Cyber Warfare*, 10.2 (2017), pp. 67-70, doi:10.4337/9781800883352.ch004.

¹¹ Eska Nia Sarinastiti and Nabilla Kusuma Vardhani, 'Internet Dan Terorisme : Menguatnya Aksi Global Cyber-Terrorism New Media', *Jurnal Gama Societa*, 1.1 (2018), p. 40, doi:10.22146/jgs.34048.



ringan, padahal dampak psikologis dan sosial dari aksi teror digital sangat luas. Hal ini memperkuat urgensi untuk mereformulasi sistem pertanggungjawaban pidana yang dapat mengakomodasi kejahatan terorisme berbasis teknologi, dengan menekankan perlunya pembuktian digital yang kuat serta pengaturan eksplisit dalam undang-undang.

Data dari Badan Nasional Penanggulangan Terorisme (BNPT) menunjukkan bahwa rekrutmen melalui internet mengalami peningkatan signifikan, terutama menyasar generasi muda yang aktif di platform digital. Strategi ini menggunakan narasi ideologis, video motivasi jihad, serta materi pembelajaran daring sebagai alat indoktrinasi.¹²

Selain itu, penggunaan e-wallet, cryptocurrency, dan sistem keuangan digital juga menjadi cara baru dalam pendanaan aksi teror. Teknologi ini membuat arus transaksi sulit dilacak secara konvensional, sehingga memberikan keuntungan taktis bagi kelompok teroris untuk menyamarkan sumber dana dan tujuan penggunaan.

Modus lainnya melibatkan peretasan situs, penyebaran konten provokatif, hingga serangan siber ke infrastruktur negara. Semua ini menunjukkan bahwa terorisme digital bukan hanya ancaman fisik, tetapi juga ancaman ideologis dan sistemik yang mengganggu stabilitas nasional serta keamanan publik.

B. Implementasi Pertanggungjawaban Pidana terhadap Pelaku Terorisme Digital

Jan Rimmelink berpendapat bahwa tujuan utama dari hukum pidana adalah menjaga keteraturan dalam sistem hukum serta memberikan perlindungan terhadap masyarakat secara menyeluruh.¹³ Dalam ranah hukum positif Indonesia, pertanggungjawaban pidana terhadap pelaku tindak pidana terorisme digital masih berpegang pada asas-asas umum hukum pidana, seperti asas legalitas, kesalahan, dan kemampuan bertanggung jawab. Namun, implementasinya menghadapi kendala teknis dan normatif akibat kompleksitas ranah siber.

Banyak kasus menunjukkan kesulitan dalam mengidentifikasi pelaku secara pasti, karena penggunaan akun anonim dan enkripsi. Hal ini menyebabkan aparat penegak hukum harus bekerja sama dengan lembaga intelijen dan penyedia platform digital untuk membongkar jejak digital pelaku. Proses ini sering kali membutuhkan waktu dan sumber daya teknologi yang besar.¹⁴

Di sisi lain, penegakan hukum terhadap pelaku terorisme digital juga berhadapan dengan isu hak asasi manusia. Prosedur penyadapan, pengawasan daring, dan penahanan berbasis bukti digital harus dilakukan dengan tetap menghormati prinsip keadilan dan non-diskriminasi. Ketimpangan penanganan dapat menimbulkan resistensi publik atau gugatan internasional.

Meski telah ada beberapa vonis pidana terhadap pelaku terorisme berbasis ITE, efektivitas penjeranya masih diragukan. Hal ini disebabkan oleh belum optimalnya integrasi hukum pidana umum dengan hukum siber dan antiterorisme, yang seharusnya membentuk satu sistem penegakan yang koheren dan komprehensif.

¹² Nugroho Prastyawan, 'Media_Sosial_dan_Radikalisme_Bagaimana_Teknologi_I', 01.04 (2023), pp. 110–15.

¹³ Didik Purwadi, Amiruddin, and Rina Khairani Pancaningrum, 'Hukum Pidana (Hukum Pidana)', *Jurnal Ketha Semaya*, 10.3 (2022), pp. 717–26.

¹⁴ Ardison Asri and others, 'Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber Di Indonesia', *Jurnal Ilmiah Hukum Dirgantara*, 15.1 (2024), pp. 1–13.



C. Evaluasi Hukum dan Rekomendasi Perbaikan Sistem Penanggulangan

Evaluasi terhadap sistem hukum saat ini menunjukkan bahwa regulasi yang ada belum sepenuhnya adaptif terhadap karakteristik kejahatan terorisme digital. UU No. 5 Tahun 2018 masih berfokus pada aspek fisik dari aksi teror, sementara UU ITE cenderung normatif tanpa penjabaran detail mengenai aktivitas teror berbasis teknologi.¹⁵

Kurangnya definisi eksplisit mengenai “terorisme digital” menyebabkan kesenjangan dalam konstruksi hukum dan pembuktian di pengadilan. Akibatnya, jaksa dan hakim sering mengandalkan interpretasi luas yang berisiko menimbulkan ketidakpastian hukum. Kondisi ini dapat dimanfaatkan oleh pelaku untuk mencari celah pembelaan atau menghindari jerat hukum.

Evaluasi terhadap regulasi yang ada menunjukkan bahwa perangkat hukum di Indonesia masih belum sepenuhnya responsif terhadap kompleksitas tindak pidana terorisme berbasis ITE. UU No. 5 Tahun 2018 lebih menitikberatkan pada tindakan fisik, seperti pengeboman atau perusakan fasilitas umum, tanpa menjabarkan bentuk serangan digital seperti penyebaran konten radikal, propaganda daring, atau rekrutmen melalui platform media sosial. Sementara itu, UU ITE cenderung bersifat normatif dan tidak secara eksplisit menyebut aktivitas terorisme digital sebagai objek pengaturannya, sehingga menimbulkan kekosongan hukum dalam praktik penegakan.

Selain ketidakjelasan pengaturan, koordinasi antarlembaga penegak hukum masih bersifat sektoral dan belum terintegrasi secara digital. Aparat kepolisian, lembaga intelijen, serta penyedia platform digital sering kali bekerja sendiri-sendiri tanpa sistem komando dan kontrol yang terkoordinasi. Padahal, bentuk kejahatan digital bersifat lintas batas dan adaptif, sehingga memerlukan respons hukum yang cepat, kolaboratif, dan didukung teknologi pemantauan yang canggih. Tanpa penguatan kelembagaan dan infrastruktur digital, efektivitas penanggulangan akan selalu tertinggal dari modus operandi pelaku.

Untuk itu, diperlukan reformulasi kebijakan hukum yang bersifat progresif dan adaptif. Pemerintah perlu merancang instrumen hukum yang secara eksplisit mengatur jenis, bentuk, dan kategori tindak pidana terorisme digital serta standar pembuktiannya. Di samping itu, perlu dibangun sistem koordinasi berbasis teknologi yang menghubungkan aparat penegak hukum, BNPT, penyedia layanan internet, dan platform media sosial dalam satu ekosistem hukum yang saling mendukung. Reformasi ini diharapkan mampu menciptakan sistem pertanggungjawaban pidana yang tidak hanya represif, tetapi juga preventif dan responsif terhadap dinamika kejahatan era digital.

Diperlukan reformulasi kebijakan hukum yang mencakup pengaturan lebih jelas mengenai bentuk, kategori, dan bukti tindak pidana terorisme berbasis ITE. Termasuk di dalamnya penguatan koordinasi antara lembaga penegak hukum dan sektor teknologi, seperti penyedia layanan digital dan platform media sosial.¹⁶

¹⁵ Ahmad Shabirin and Arjun, ‘Asas Legalitas Dalam Penanggulangan Radikalisme Online: Perspektif Hukum Pidana Indonesia’, *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 1.3 (2025), pp. 333–44, doi:10.63822/czsz4m55.

¹⁶ Dwi Nugroho Marsudianto and Herman Bakir, ‘Reconstruction of Criminal Law to Address Cyber Terrorism in Indonesia’, *Journal of Social Science (JoSS)*, 3.11 (2024), pp. 1962–68, doi:10.57185/joss.v3i11.382.



Rekomendasi yang dapat diajukan antara lain adalah penyusunan regulasi khusus mengenai cyber terrorism, peningkatan kapasitas penyidik dan penuntut dalam digital forensics, serta integrasi sistem pengawasan daring berbasis artificial intelligence untuk mendeteksi potensi teror sejak dini. Pendekatan preventif dan kolaboratif menjadi kunci dalam menciptakan sistem hukum pidana yang tangguh terhadap ancaman digital.

Kesimpulan

Tindak pidana terorisme berbasis ITE merupakan bentuk kejahatan modern yang memanfaatkan kemajuan teknologi informasi untuk menyebarkan paham radikal, merekrut anggota, serta merencanakan dan mendanai aksi kekerasan. Pola ini tidak hanya mengancam keamanan negara secara fisik, tetapi juga merusak stabilitas sosial dan ideologi bangsa melalui penetrasi digital yang sulit dikendalikan dengan pendekatan hukum konvensional.

Pertanggungjawaban pidana terhadap pelaku terorisme digital masih menghadapi tantangan baik secara teknis maupun yuridis. Meskipun instrumen hukum seperti Undang-Undang Terorisme dan Undang-Undang ITE telah ada, masih terdapat kekosongan norma dan disharmoni dalam penegakan hukum yang menyebabkan proses peradilan tidak selalu efektif. Kompleksitas pembuktian di dunia maya serta keterbatasan sumber daya penegak hukum menjadi hambatan nyata dalam menetapkan kesalahan pelaku secara sah dan meyakinkan.

Oleh karena itu, perlu dilakukan pembaruan hukum yang menyeluruh melalui perumusan regulasi yang secara eksplisit mengatur tindak pidana terorisme digital, peningkatan kapasitas aparat penegak hukum di bidang digital forensik, serta penguatan kerja sama antarinstansi dan sektor privat. Langkah-langkah ini penting untuk memastikan bahwa sistem hukum pidana nasional mampu menghadapi tantangan kejahatan berbasis teknologi dengan adil, efektif, dan berorientasi pada perlindungan masyarakat secara menyeluruh.

Daftar Pustaka

- Abdullah Husein Al Aziz, and Zainudin Hasan, 'Pertanggungjawaban Pidana Pelaku Tindak Pidana Pengancaman Dengan Revenge Porn Dalam Era Digital Di Kota Bandar Lampung', *Jurnal Hukum, Politik Dan Ilmu Sosial*, 3.4 (2024), pp. 341–55, doi:10.55606/jhpis.v3i4.4476
- Ahmad Shabirin, and Arjun, 'Asas Legalitas Dalam Penanggulangan Radikalisme Online: Perspektif Hukum Pidana Indonesia', *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 1.3 (2025), pp. 333–44, doi:10.63822/czsz4m55
- Asri, Ardison, and others, 'Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber Di Indonesia', *Jurnal Ilmiah Hukum Dirgantara*, 15.1 (2024), pp. 1–13
- Bastian, Muhammad Arkhan Maulana, Rudy Sutanto, and Raden Ruli Basuni, 'Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Dalam Pencegahan Cyberterrorism', *Jurnal Hukum Mimbar Justitia*, 10.2 (2025), p. 430, doi:10.35194/jhmj.v10i2.4997
- Hasan, Zainudin. 2025. "Sistem Peradilan Pidana Penjara", CV. Alinea Edumedia, Cilacap, hlm. 5.



- Hasan, Zainudin. 2025. "*Penegak Hukum Dan Penegakan Hukum Di Indonesia*", Universitas Bandar Lampung (UBL) Press, Bandar Lampung, hlm. 11.
- Iqbal, Muhammad, Heru Juli Ardie, and Zainudin Hasan, 'Analisis Hukum Dalam Melacak Jejak Digital Dan Memahami Tindak Pidana Pencucian Uang Dalam Era Teknologi', *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syaria'h*, 5 (2024), pp. 286–98, doi:10.24252/iqtishaduna.vi.43802
- Jacob, Frank, 'Cyber Terrorism', *Encyclopedia of Cyber Warfare*, 10.2 (2017), pp. 67–70, doi:10.4337/9781800883352.ch004
- Marsudianto, Dwi Nugroho, and Herman Bakir, 'Reconstruction of Criminal Law to Address Cyber Terrorism in Indonesia', *Journal of Social Science (JoSS)*, 3.11 (2024), pp. 1962–68, doi:10.57185/joss.v3i11.382
- Nugroho Prastyawan, 'Media_Sosial_dan_Radikalisme_Bagaimana_Teknologi_I', 01.04 (2023), pp. 110–15
- Purwadi, Didik, Amiruddin, and Rina Khairani Pancaningrum, 'Hukum Pidana (Hukum Pidana)', *Jurnal Ketha Semaya*, 10.3 (2022), pp. 717–26
- Sarinastiti, Eska Nia, and Nabilla Kusuma Vardhani, 'Internet Dan Terorisme : Menguatnya Aksi Global Cyber-Terrorism New Media', *Jurnal Gama Societa*, 1.1 (2018), p. 40, doi:10.22146/jgs.34048
- Sudut, Cyber-terrorism Dari, and Pandang Hukum, 'Cyber-Terrorism Dari Sudut Pandang Hukum Pidana Indonesia', pp. 1–13
- Wahyudi, Yusril Iman, Nining Haslinda Zainal, and Ade Ferry Afrisal, 'Indeks Kepuasan Masyarakat Terhadap Pelayanan Perizinan Berbasis Aplikasi OSS Di Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Kabupaten Pinrang', *Publician: Journal of Public Service, Public Policy, and Administrastion*, 3.1 (2024), pp. 44–50, doi:10.56326/jp.v3i1.4135