ISTISHLAH: JURNAL HUKUM ISLAM, 03 (01), 2025: 46-57
Available online at: https://jurnal.uinsu.ac.id/index.php/istishlah
DOI: http://dx.doi.org/10.30821/istishlah.v3i1.25977
P-ISSN: XXXX-XXXX, E-ISSN: XXXX-XXXX

KESENJANGAN HUKUM DALAM PENANGGULANGAN TERORISME DI INDONESIA (ANALISIS TERHADAP ANCAMAN SIBER DAN RADIKALISASI ONLINE)

Usman Betawi
Sekolah Tinggi Agama Islam Darul Arafah, Indonesia
email: usbetawi@gmail.com

Ahmat
Sekolah Tinggi Ilmu Kesehatan Binalita Sudama Medan, Indonesia
email: ahmadfaury28@gmail.com

Abstract: *Terrorism is an extraordinary crime that not only threatens national security but also disrupts social, political, and economic stability. In recent decades, terrorism has significantly transformed through digital platforms, including online radicalization and cyber terrorism. Indonesia, with its large number of internet users, has become a strategic target for extremist groups. Although Law No. 5 of 2018 on the Eradication of Terrorism and the Electronic Information and Transactions Law (ITE Law) provide a legal basis, significant legal and technical gaps remain in addressing the transnational, anonymous, and untraceable nature of digital terrorism. This study examines how effective Indonesia's legal framework is in combating cyber terrorism and to what extent law enforcement institutions can respond to these challenges. The objectives are to identify substantive and procedural legal gaps, assess institutional technical capacity, and provide policy recommendations to strengthen legal responses. The research adopts a normative juridical method with a statute approach and qualitative analysis of legal documents, legislation, and policy papers. The findings reveal that despite the expanded definition of terrorism in the 2018 Law, it does not explicitly include online radicalization, digital propaganda, or cyber-based funding. Furthermore, limited digital forensic capacity, weak interagency coordination, and the absence of specific regulations on digital surveillance hinder effective enforcement. In conclusion, countering digital terrorism in Indonesia requires adaptive legal reforms, strengthened technical capabilities, and more comprehensive interagency and international cooperation.*
Keywords: Cyber Terrorism, Online Radicalization, Legal Gaps, Law Enforcement, Indonesia

Abstrak: Terorisme merupakan kejahatan luar biasa yang tidak hanya mengancam keamanan nasional, tetapi juga merusak tatanan sosial, politik, dan ekonomi. Dalam dekade terakhir, ancaman terorisme mengalami transformasi signifikan melalui ruang digital, meliputi radikalisasi online dan terorisme siber. Indonesia, dengan jumlah pengguna internet yang sangat besar, menjadi target strategis kelompok ekstremis. Namun, meskipun telah lahir UU No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme serta UU ITE, terdapat kesenjangan hukum dan teknis dalam menghadapi ancaman digital yang bersifat transnasional, anonim, dan sulit dilacak. Permasalahan yang dikaji dalam penelitian ini adalah bagaimana efektivitas kerangka hukum nasional dalam menanggulangi terorisme siber dan sejauh mana kapasitas institusi penegak hukum mampu merespons tantangan tersebut. Tujuan penelitian adalah mengidentifikasi celah hukum substantif maupun prosedural, menilai kapasitas teknis institusional, serta memberikan rekomendasi kebijakan untuk memperkuat respons hukum. Metode penelitian yang digunakan adalah yuridis normatif dengan statute approach serta analisis kualitatif berbasis studi literatur, peraturan perundang-undangan, dan dokumen kebijakan. Hasil penelitian menunjukkan bahwa meskipun UU Terorisme 2018 telah memperluas definisi terorisme, ketentuan ini belum mengakomodasi secara eksplisit aktivitas radikalisasi online, propaganda digital, dan pendanaan siber. Di sisi lain, keterbatasan digital forensics, lemahnya koordinasi antar lembaga, serta ketiadaan regulasi spesifik mengenai penyadapan digital menambah hambatan. Kesimpulannya, penanggulangan

terorisme digital di Indonesia membutuhkan reformasi hukum yang adaptif, penguatan kapasitas teknis, serta mekanisme koordinasi lintas lembaga dan internasional yang lebih komprehensif.
Kata kunci: Terorisme Siber, Radikalisasi Online, Kesenjangan Hukum, Penegakan Hukum, Indonesia

1. PENDAHULUAN

Terorisme, sebagai salah satu bentuk kejahatan luar biasa (extraordinary crime), telah menjadi ancaman global yang tidak hanya mengganggu stabilitas keamanan nasional, tetapi juga merusak tatanan sosial, ekonomi, dan politik di berbagai negara.[1] Di Indonesia, sebagai negara dengan keragaman etnis, agama, dan budaya yang sangat tinggi, ancaman terorisme memiliki potensi besar untuk memecah belah persatuan bangsa. Sejak awal abad ke-21, Indonesia telah mengalami sejumlah serangan teroris yang menewaskan ratusan korban, seperti pengeboman Bali pada tahun 2002 dan 2005, pengeboman JW Marriott dan Ritz-Carlton di Jakarta pada 2009, serta serangan di Mako Brimob pada 2018. Serangan-serangan tersebut menunjukkan bahwa terorisme bukan hanya persoalan keamanan, melainkan juga tantangan multidimensi yang mencakup aspek ideologi, sosial, ekonomi, dan hukum.

Namun, dalam satu dekade terakhir, bentuk ancaman terorisme telah mengalami transformasi yang signifikan. Perkembangan teknologi informasi dan komunikasi (TIK) yang begitu pesat telah membuka ruang baru bagi kelompok teroris untuk beroperasi di luar batas geografis dan temporal. Dunia maya yang mencakup media sosial, platform digital, forum daring, aplikasi perpesanan instan, dan bahkan dark web telah menjadi medan strategis bagi penyebaran propaganda, perekrutan anggota, penggalangan dana, koordinasi aksi, serta pelatihan ideologis. Fenomena ini dikenal sebagai radikalisasi online dan ancaman siber terorisme (cyber terrorism). Dalam konteks ini, terorisme tidak lagi terbatas pada aksi kekerasan fisik, tetapi juga meliputi penyebaran narasi kebencian, doktrin ekstremis, dan ajakan kekerasan melalui saluran digital yang sulit dilacak dan dikendalikan.[2]

Indonesia, sebagai negara dengan jumlah pengguna internet tertinggi di Asia Tenggara dengan lebih dari 200 juta pengguna aktif pada tahun 2023 menjadi target empuk bagi kelompok teroris untuk melakukan ekspansi ideologis secara daring. Data dari Buletin APBN menunjukkan bahwa Indonesia menempati urutan ke 35 dari 135 yang terdampak terorisme. Selain itu, masifnya penggunaan internet saat ini turut menjadi tantangan tersendiri. Internet menjadi media yang memudahkan para teroris mendoktrin generasi muda. Kepala Badan Nasional Penanggulangan Terorisme (BNPT) menyebutkan bahwa kasus wanita muda yang menyerang Mabes POLRI pada 2021 lalu diduga karena terpapar ideologi

[1] Aulia Rosa Nasution, "Penegakan Hukum Terhadap Tindakan Terorisme sebagai 'Extraordinary Crime' dalam Perspektif Hukum Internasional dan Nasional," *LWSA Conference Series* 1 (2018): 8.

[2] Agung Sukoco dkk., "Media, Globalisasi dan Ancaman Terorisme," *Journal of Terrorism Studies* 3, no. 2 (2021): 2.

Islamic State of Iraq and Syria (ISIS) dari internet.[3] Selain itu, platform seperti Telegram, YouTube, Facebook, dan bahkan TikTok telah dimanfaatkan untuk menyebarkan konten yang mendukung ideologi kelompok seperti ISIS, Al-Qaeda, dan Jamaah Ansharut Daulah (JAD). Sifat anonim, cepat, dan luas jangkauan dari media digital membuat upaya pencegahan dan penindakan menjadi semakin kompleks.

Dalam merespons ancaman ini, Indonesia telah melakukan sejumlah langkah hukum dan kebijakan. Salah satu tonggak penting adalah lahirnya Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme. UU ini dianggap sebagai langkah maju karena memperluas definisi terorisme, memperkuat kewenangan aparat penegak hukum dalam pencegahan, serta mengatur sanksi bagi mereka yang bergabung dengan organisasi teroris di luar negeri atau mengikuti pelatihan militer ekstremis. Selain itu, UU ini juga mengakomodasi aspek de-radikalisasi dan reintegrasi teroris yang telah menjalani hukuman.[4]

Namun, meskipun UU Terorisme 2018 relatif komprehensif dalam menghadapi ancaman konvensional, kesenjangan hukum yang signifikan tetap terjadi dalam konteks ancaman siber dan radikalisasi online.[5] Selain itu, kerangka hukum nasional belum sepenuhnya mampu menangani sifat lintas batas (transnational) dari dunia maya, di mana konten radikal bisa diunggah dari server di luar negeri, menggunakan virtual private network (VPN), atau dienkripsi sehingga menyulitkan proses penyelidikan dan pengumpulan bukti. Kondisi ini diperparah oleh keterbatasan kapasitas teknis dan institusional. Lembaga penegak hukum seperti POLRI, BNPT, dan Kejaksaan Agung sering kali menghadapi hambatan dalam hal digital forensics, pelacakan IP address, dan interpretasi konten digital yang bernuansa ideologis. Koordinasi antarlembaga juga masih belum optimal, baik secara teknis maupun birokratis. Di tingkat internasional, meskipun Indonesia telah terlibat dalam sejumlah kerja sama seperti Global Counterterrorism Forum (GCTF) dan ASEANAPOL, kerangka hukum harmonisasi untuk menangani terorisme siber masih sangat terbatas. Akibatnya, banyak pelaku yang lolos dari jerat hukum karena ketiadaan dasar hukum yang memadai atau keterlambatan respons negara.[6]

Berdasarkan urgensi dan kompleksitas masalah tersebut, penelitian ini dirancang untuk menganalisis secara kritis kesenjangan hukum dalam penanggulangan terorisme di Indonesia, khususnya dalam menghadapi ancaman siber dan radikalisasi online. Tujuan utama penelitian ini adalah untuk

[3] Tio Riyono, "Perkembangan Terorisme dan Anggaran Penanganan Terorisme di Indonesia," *Buletin APBN* 7, no. 2 (2022): 7.

[4] Folman P Ambarita, "Penanggulangan Tindak Pidana Terorisme," *Binamulia Hukum* 7, no. 2 (2018): 151.

[5] Ahmad Sholihin dan Heri Kurnia, "Internet Sebagai Media Peneybaran Ideologi Radikal: Dampak, Tantangan, dan Upaya Penanggulangannya," *Academy of Social Science and Global Citizenship Journal* 3, no. 1 (2023): 26.

[6] Danang Enggartyasto dan Irwan Hafid, "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia," *Lex Renaissance* 1, no. 7 (2022): 89.

mengidentifikasi celah-celah hukum yang ada dalam sistem perundang-undangan nasional, mengevaluasi efektivitas penegakan hukum dalam konteks digital, serta memberikan rekomendasi kebijakan yang dapat memperkuat kapasitas hukum dan institusional dalam menghadapi terorisme di ruang siber.

Secara lebih spesifik, penelitian ini bertujuan untuk menganalisis ketentuan hukum nasional yang relevan dengan ancaman terorisme siber dan radikalisasi online, termasuk UU Terorisme 2018, UU Informasi dan Transaksi Elektronik (ITE) dan peraturan turunan lainnya, serta memberikan rekomendasi kebijakan yang berbasis bukti untuk memperbaiki kerangka hukum dan institusional dalam konteks ancaman digital.

Manfaat penelitian ini bersifat ganda: akademis dan praktis. Secara akademis, penelitian ini akan memperkaya kajian hukum pidana, keamanan nasional, dan hukum siber di Indonesia. Penelitian ini juga akan memberikan kontribusi terhadap literatur tentang counter-terrorism law dalam konteks negara berkembang yang menghadapi dualitas antara kebebasan digital dan keamanan negara. Secara praktis, temuan penelitian ini dapat menjadi dasar bagi pembuat kebijakan—seperti DPR, Kementerian Hukum dan HAM, BNPT, dan POLRI—dalam merancang revisi undang-undang, menyusun regulasi turunan, atau memperkuat kapasitas institusional. Selain itu, hasil penelitian ini juga dapat digunakan oleh lembaga masyarakat sipil (LSM), akademisi, dan media sebagai bahan edukasi publik mengenai bahaya radikalisasi online dan pentingnya penegakan hukum yang seimbang.

Penelitian ini memperluas dan memperdalam pengetahuan di bidang hukum dan keamanan nasional dengan beberapa cara. Pertama, penelitian ini memberikan analisis empiris terbaru mengenai implementasi UU Terorisme 2018 dalam konteks digital—sesuatu yang masih jarang dilakukan oleh peneliti sebelumnya. Kedua, penelitian ini mengintegrasikan perspektif hukum, teknologi, dan kebijakan publik, sehingga memberikan pendekatan multidisipliner yang lebih komprehensif. Ketiga, penelitian ini mengangkat isu-isu yang belum banyak dibahas secara mendalam, seperti peran cryptocurrency dalam pendanaan terorisme daring, atau penggunaan deep learning oleh kelompok teroris untuk menyebarkan propaganda.

Selain itu, penelitian ini juga memperjelas batas antara kebebasan digital dan keamanan negara isu yang semakin relevan di tengah maraknya pembatasan konten di bawah dalih pencegahan terorisme. Dengan memberikan rekomendasi yang seimbang antara efektivitas hukum dan perlindungan HAM, penelitian ini berkontribusi pada diskusi kebijakan yang lebih arif dan berbasis data.

2. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis normatif dengan pendekatan statute approach untuk menganalisis kerangka hukum yang berlaku dalam penanggulangan terorisme siber dan radikalisasi online di Indonesia. Pendekatan ini dipilih karena fokus utama penelitian berada pada eksistensi, struktur, dan substansi peraturan perundang-

undangan sebagai acuan utama dalam mengevaluasi kesenjangan hukum yang terjadi.[7]

Dalam kerangka ini, sumber data bersifat primer dan sekunder, di mana data primer mencakup peraturan perundang-undangan nasional seperti Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh UU Nomor 19 Tahun 2016, serta peraturan pelaksana turunannya seperti Peraturan Pemerintah dan Peraturan Presiden yang relevan. Selain itu, putusan pengadilan yang berkaitan dengan kasus terorisme berbasis digital juga dijadikan bagian dari data primer untuk melihat praktik penafsiran hukum oleh lembaga peradilan. Sementara itu, data sekunder diperoleh dari berbagai literatur hukum, jurnal ilmiah, laporan resmi instansi pemerintah seperti BNPT dan KOMINFO, dokumen kebijakan nasional dan internasional, serta hasil penelitian terdahulu yang membahas isu terorisme, keamanan siber, dan hak asasi manusia.

Pengumpulan data dilakukan melalui studi dokumen dan kepustakaan secara sistematis, dengan prosedur yang mencakup identifikasi dokumen hukum utama, pelacakan perkembangan regulasi terkait, serta analisis kritis terhadap konsistensi, kelengkapan, dan relevansi norma hukum terhadap fenomena ancaman siber.

Teknik analisis data dilakukan secara kualitatif dengan metode analisis isi (content analysis) yang bertujuan mengidentifikasi pola, ketidakkonsistenan, dan celah dalam ketentuan hukum yang ada, serta mengevaluasi sejauh mana kerangka hukum mampu merespons dinamika modus operandi terorisme di ruang digital.[8] Proses analisis dilakukan secara tematik dengan membandingkan ketentuan hukum satu sama lain, menelaah konteks historis dan tujuan legislasi, serta menilai implikasi praktis dari penerapan norma tersebut dalam penegakan hukum. Melalui pendekatan ini, penelitian mampu memberikan gambaran komprehensif mengenai kesenjangan hukum substantif dan prosedural, sekaligus menjawab pertanyaan penelitian mengenai efektivitas kerangka hukum dan kapasitas institusional dalam menghadapi ancaman terorisme siber, tanpa bergantung pada data empiris dari wawancara atau survei, sesuai dengan karakteristik penelitian yuridis normatif yang berfokus pada doktrin dan struktur hukum formal.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Kesenjangan Hukum Substantif Dan Prosedural Dalam Penanggulangan Terorisme Siber di Indonesia

Terorisme di era digital telah mengalami transformasi yang sangat signifikan, tidak lagi terbatas pada aksi kekerasan fisik yang terlokalisasi, tetapi telah berkembang menjadi fenomena yang bersifat transnasional, anonim, dan

[7] Geofani Milthree Saragih, *Metode Penelitian Hukum* (Sada Kurnia Pustaka, 2023), 126.

[8] Missiliana Riasnugrahani dan Priska Analya, *Metode Penelitian Kualitatif* (Ideas Publishing, 2023), 1.

berbasis teknologi informasi. Ancaman siber terorisme (cyber terrorism) dan radikalisasi online menjadi bentuk baru dari ekspresi kekerasan ideologis yang memanfaatkan ruang digital sebagai alat propaganda, perekrutan, pendanaan, dan koordinasi.[9] Di Indonesia, sebagai negara dengan penetrasi internet yang tinggi dengan lebih dari 200 juta pengguna aktif pada tahun 2023 menurut data Wearsocial, ruang siber menjadi medan yang sangat rentan terhadap infiltrasi ideologi ekstrem.[10] Namun, meskipun pemerintah telah mengambil langkah hukum penting melalui Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme (selanjutnya disebut UU Terorisme 2018), serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah oleh UU Nomor 19 Tahun 2016, kesenjangan hukum substantif dan prosedural masih terbuka lebar dalam menghadapi ancaman terorisme berbasis siber. Kesenjangan ini bukan hanya terletak pada ketiadaan norma yang eksplisit, tetapi juga pada tumpang tindih, ambiguitas, dan ketidakmampuan hukum nasional untuk menangkap dinamika modus operandi terorisme di dunia maya yang bersifat cepat, lintas batas, dan anonim.

UU Terorisme 2018 memang membawa perubahan mendasar dalam pendekatan hukum terhadap terorisme. Salah satu kemajuan utama adalah perluasan definisi terorisme dalam Pasal 1 ayat 2, yang menyatakan bahwa terorisme adalah "perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara luas, yang dapat menimbulkan korban massa secara tidak wajar, dan/atau menghancurkan fasilitas publik atau fasilitas vital tertentu, dengan motif ideologi, politik, atau gangguan keamanan".[11] Perluasan ini memungkinkan penjeratan terhadap tindakan yang belum mencapai tahap eksekusi, seperti pelatihan militer, rekrutmen, dan pendanaan. Namun, yang menjadi persoalan kritis adalah bahwa definisi ini masih berfokus pada dimensi fisik dan material, sementara aktivitas terorisme di dunia siber seperti penyebaran propaganda, ujaran kebencian, atau penggalangan dana digital tidak secara eksplisit dianggap sebagai bagian dari tindak pidana terorisme. Akibatnya, banyak pelaku yang menyebarkan konten radikal di media sosial hanya dijerat dengan UU ITE, khususnya Pasal 28 ayat (2) tentang ujaran kebencian atau Pasal 45 Ayat 1 tentang konten provokatif, yang sanksinya jauh

[9] Aloysius Harry Mukti dan Yohanes Febrian, "Kesiapan Mendeteksi Kegiatan Pendanaan Terorisme Dalam Era Digital Keuangan (Fintech)," *Hukum Pidana dan Pembangunan HUkum* 1, no. 1 (2018): 4.

[10] Ahmad Thoriq Akhsan Ramdhani dan Agung Rashif Madani, "Aktivitas Gen-Z Terhadap Pengembangan UMKM Melalui Digitalisasi (Studi Kasus di Wilayah Kapanewon Moyudan)," *Aplikasia: Jurnal Aplikasi Ilmu-Ilmu Agama* 23, no. 2 (2023): 162.

[11] Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang (2018).

lebih ringan dibandingkan tindak pidana terorisme yang bisa mencapai hukuman mati.[12]

Ketidakselarasan ini menciptakan celah hukum yang signifikan, di mana pelaku yang secara ideologis dan operasional mendukung terorisme tetapi tidak melakukan aksi fisik kekerasan, sulit dijerat sebagai pelaku terorisme. Lebih lanjut, UU ITE sendiri tidak dirancang untuk menangani ancaman terorisme, melainkan lebih fokus pada perlindungan konsumen, keamanan transaksi elektronik, dan pencegahan penyebaran informasi palsu atau konten asusila. Meskipun Pasal 28 ayat (2) UU ITE dapat digunakan untuk menjerat penyebaran konten yang mengandung kebencian berdasarkan SARA, ketentuan ini tidak cukup kuat untuk menangani konten yang bernuansa ideologis-ekstremis seperti doktrin takfiri, ajakan jihad, atau justifikasi kekerasan terhadap negara. Selain itu, interpretasi yang terlalu luas terhadap UU ITE justru berpotensi melanggar hak asasi manusia, khususnya kebebasan berekspresi, sebagaimana dijamin dalam Pasal 28 UUD 1945. Banyak kasus di mana aktivis, jurnalis, atau warga biasa dijerat dengan UU ITE hanya karena mengkritik kebijakan pemerintah, sementara pelaku radikalisasi online yang benar-benar membahayakan keamanan nasional lolos dari jerat hukum karena ketiadaan norma yang spesifik. Kondisi ini menciptakan ketidakadilan hukum dan distorsi prioritas penegakan hukum.[13]

Dari sisi prosedural, kesenjangan hukum juga terlihat jelas dalam proses pengumpulan, penyimpanan, dan pemeriksaan alat bukti elektronik. Meskipun UU ITE mengatur tentang digital evidence dalam Pasal 5 ayat (1) dan Pasal 30, implementasinya masih sangat lemah. Penyidik sering kali menghadapi kesulitan dalam mendapatkan data dari penyedia layanan digital (seperti Meta, Google, atau Telegram), terutama karena banyak platform tersebut berbasis di luar negeri dan tidak memiliki kantor perwakilan resmi di Indonesia. Selain itu, tidak semua kepolisian daerah memiliki unit digital forensik yang memadai, sehingga proses verifikasi dan autentikasi bukti sering dilakukan oleh pusat, menyebabkan keterlambatan dan akumulasi beban kerja.

Selain itu, UU Terorisme 2018 tidak mengatur secara eksplisit tentang kewenangan penyadapan atau akses ke data terenkripsi, yang merupakan alat krusial dalam mengungkap jaringan teroris daring. Di negara-negara seperti Amerika Serikat atau Inggris, undang-undang khusus seperti Investigatory Powers Act memberikan kewenangan luas kepada badan intelijen untuk melakukan penyadapan dalam konteks ancaman terorisme.[14] Di Indonesia, meskipun ada

[12] Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2024).

[13] Ainun Sakinah Durhan, "Pengaruh Terpaan Informasi Kasus UU ITE Terhadap Kebebasan Berekspresi Pengguna Media Sosial di Kota Makassar" (Tesis, Universitas Hasanuddin, 2021), 31.

[14] Mety Rahmawati, "Perbandingan Pengaturan Perlindungan Hukum Bagi Penyidik, Penuntut Umum, Hakim, Advokat, Pelapor, Ahli, Saksi Dan Petugas Pemasyakatan Beserta Keluarganya Dalam Perkara Terorisme Indonesia Dan Amerika Serikat," *Hukum Pidana dan Pembangunan HUkum* 1, no. 1 (2018): 2.

UU Nomor 11 Tahun 2009 tentang Keterbukaan Informasi Publik dan UU Nomor 2 Tahun 2022 tentang Intelijen Negara, tidak ada regulasi yang secara spesifik mengatur penyadapan digital dalam konteks terorisme siber. Akibatnya, aparat sering kali harus menggunakan kewenangan umum yang tidak memadai, atau melakukan penyadapan tanpa dasar hukum yang jelas, yang berpotensi melanggar hak privasi warga negara.

Selain aspek substantif dan prosedural, kesenjangan juga terjadi dalam harmonisasi antarperaturan. UU Terorisme, UU ITE, UU Intelijen, dan UU Keamanan Nasional (UU Nomor 7 Tahun 2014) seharusnya saling melengkapi, tetapi dalam praktiknya sering terjadi tumpang tindih dan konflik kewenangan. Misalnya, BNPT memiliki kewenangan pencegahan terorisme, tetapi tidak memiliki akses langsung ke data digital yang dikendalikan oleh KOMINFO atau POLRI. KOMINFO memiliki kewenangan memblokir konten, tetapi tidak dapat melakukan penyelidikan kriminal. POLRI memiliki kewenangan penyidikan, tetapi sering kali terlambat merespons karena kurangnya kapasitas teknis. Tanpa kerangka hukum yang mengatur koordinasi dan data sharing antarlembaga secara sah dan terstruktur, penanggulangan terorisme siber menjadi fragmentatif dan tidak efisien.

Rekomendasi hukum yang dapat diajukan untuk menutup kesenjangan ini antara lain: (1) amandemen UU Terorisme 2018 untuk secara eksplisit memasukkan aktivitas radikalisasi online, penyebaran propaganda, dan pendanaan digital sebagai bagian dari tindak pidana terorisme, dengan tetap mempertimbangkan prinsip proportionality dan due process; (2) pembentukan undang-undang khusus tentang keamanan siber nasional yang mengatur kewenangan penyadapan, akses data, dan kerja sama internasional dalam konteks ancaman terorisme; (3) penguatan UU ITE dengan menambahkan pasal khusus tentang penyalahgunaan media digital untuk mendukung organisasi teroris, dilengkapi dengan sanksi yang setara dengan UU Terorisme; (4) pembentukan lembaga pengawas independen yang berwenang mengawasi penggunaan kewenangan digital oleh aparat penegak hukum; dan (5) harmonisasi peraturan antarlembaga melalui Peraturan Presiden atau Peraturan Bersama Menteri yang mengatur alur koordinasi, pembagian tugas, dan mekanisme real-time data sharing.

Tanpa perbaikan mendasar terhadap kerangka hukum ini, Indonesia akan terus tertinggal dalam menghadapi ancaman terorisme di era digital. Hukum harus mampu beradaptasi dengan perkembangan teknologi, bukan hanya sebagai alat represif, tetapi juga sebagai instrumen pencegahan yang proaktif, seimbang, dan berbasis HAM. Karena jika hukum terus tertinggal, maka ruang siber akan menjadi wilayah tak bertuan yang dimanfaatkan oleh kelompok ekstremis untuk melemahkan negara dari dalam.

3.2 Efisiensi Institusi Penegak Hukum Dan Kerja Sama Antarlembaga Dalam Penanggulangan Terorisme Siber

Efektivitas penanggulangan terorisme siber di Indonesia tidak hanya ditentukan oleh kualitas peraturan hukum, tetapi juga oleh kapasitas institusional,

koordinasi antarlembaga, dan kesiapan operasional dalam menghadapi ancaman yang bersifat kompleks, dinamis, dan transnasional. Meskipun Indonesia telah memiliki sejumlah lembaga strategis seperti Badan Nasional Penanggulangan Terorisme (BNPT), Kepolisian Republik Indonesia (POLRI), Kementerian Komunikasi dan Informatika (KOMINFO), Kejaksaan Agung, serta Badan Intelijen Negara (BIN), koordinasi dan sinergi antarlembaga ini masih jauh dari optimal, baik dari sisi teknis, birokratis, maupun strategis. Keterbatasan ini menyebabkan respons terhadap ancaman terorisme siber menjadi lambat, terfragmentasi, dan sering kali tidak komprehensif. Dalam hal ini, efisiensi institusi bukan hanya soal kewenangan, tetapi juga tentang kemampuan teknis, interoperabilitas sistem, dan budaya kerja sama yang kuat antarinstansi. Salah satu tantangan utama adalah ketidakseimbangan kapasitas teknis antarlembaga. BNPT, meskipun ditunjuk sebagai koordinator nasional penanggulangan terorisme, memiliki keterbatasan dalam sumber daya digital forensik dan analisis data besar (big data analytics). Sebagian besar kemampuan analisis konten digital masih bergantung pada POLRI, khususnya Divisi Teknologi Informasi dan Komunikasi (Div TI) dan Badan Reserse Kriminal (Bareskrim).

Selain kapasitas teknis, keterbatasan sumber daya manusia (SDM) yang ahli di bidang keamanan siber dan terorisme digital juga menjadi hambatan besar. Menurut data BNPT, jumlah tenaga ahli digital forensik dan analis intelijen siber di seluruh Indonesia masih cenderung kurang, sementara jumlah konten radikal yang terdeteksi mencapai ratusan ribu per tahun. Kondisi ini membuat proses monitoring, takedown, dan investigation menjadi sangat selektif dan tidak menyeluruh.[15] Akibatnya, banyak konten radikal yang lolos dari deteksi, terutama yang menggunakan kode, simbol, atau bahasa gaul (slang) untuk menghindari keyword filtering yang digunakan oleh sistem KOMINFO. Selain itu, kurangnya pelatihan berkelanjutan bagi penyidik dan jaksa dalam menghadapi kasus terorisme digital menyebabkan kesalahan interpretasi bukti atau tuntutan yang lemah di pengadilan.

Untuk meningkatkan efisiensi institusi, diperlukan transformasi kelembagaan yang mendasar. Pertama, pembentukan Pusat Keamanan Siber Nasional (National Cyber Security Center/NCSC) yang berada di bawah koordinasi langsung Presiden, dengan mandat untuk mengintegrasikan seluruh kapasitas digital dari BNPT, POLRI, KOMINFO, BIN, dan TNI. Pusat ini harus dilengkapi dengan sistem command and control terpadu, data lake nasional untuk intelijen digital, dan cyber fusion center yang mampu melakukan analisis real-time terhadap ancaman. Kedua, penguatan kapasitas SDM melalui pelatihan berkelanjutan, rekrutmen ahli siber, dan kerja sama dengan institusi akademik dan swasta. Program seperti Cyber Resilience Fellowship atau Digital Forensics Certification harus diwajibkan bagi

[15] Claudia Nuke Irviana dan Roy Valiant Salomo, "Analisis Pengembangan Kapasitas Organisasi Di Direktorat Tindak Pidana Siber (DITTIPIDSIBER), Badan Reserse Kriminal Polri (BARESKRIM POLRI)," *Media Bina Ilmiah* 15, no. 11 (2021): 5690.

penyidik dan jaksa yang menangani kasus terorisme digital. Ketiga, pembuatan protokol koordinasi yang mengikat secara hukum, misalnya melalui Peraturan Presiden, yang mengatur alur komunikasi, pembagian tugas, dan mekanisme data sharing antarlembaga. Protokol ini harus mencakup standard operating procedure (SOP) untuk penanganan kasus siber terorisme, termasuk waktu respons, format laporan, dan mekanisme eskalasi. Keempat, penguatan kerja sama internasional melalui diplomasi siber, termasuk penandatanganan bilateral cyber agreements dengan negara-negara mitra strategis, serta penguatan peran Indonesia dalam forum ASEAN untuk mendorong harmonisasi hukum siber regional. Kelima, pemberdayaan sektor swasta dan masyarakat sipil sebagai mitra dalam deteksi dini, melalui program public-private partnership (PPP) dalam bentuk cyber watch atau community reporting system.

Tanpa langkah-langkah strategis ini, Indonesia akan terus rentan terhadap ancaman terorisme siber. Efisiensi institusi bukan sekadar soal struktur, tetapi tentang kemampuan sistem untuk merespons secara cepat, akurat, dan terpadu. Dalam perang melawan terorisme digital, kemenangan tidak ditentukan oleh jumlah pasukan, tetapi oleh kecepatan informasi, ketepatan analisis, dan soliditas kerja sama. Oleh karena itu, reformasi kelembagaan adalah keniscayaan, bukan pilihan.

4. KESIMPULAN

Hubungan antara kerangka hukum nasional, kapasitas institusional, dan dinamika ancaman terorisme siber di Indonesia menunjukkan bahwa ketidakselarasan antara regulasi yang ada dengan realitas modus operandi terorisme di ruang digital telah menciptakan celah strategis yang dapat dimanfaatkan oleh kelompok ekstremis. Temuan penelitian mengungkap bahwa meskipun UU Terorisme 2018 dan UU ITE memberikan dasar hukum yang relatif kuat dalam menangani kejahatan konvensional, keduanya gagal merespons secara memadai terhadap kompleksitas ancaman yang bersifat transnasional, anonim, dan berbasis teknologi. Kesenjangan substantif terlihat dari ketiadaan definisi yang eksplisit mengenai radikalisasi online, propaganda digital, dan pendanaan siber sebagai bagian integral dari tindak pidana terorisme, sehingga banyak aktivitas yang secara faktual mendukung jaringan teroris hanya dijerat dengan pasal-pasal yang lebih ringan dan tidak relevan secara kontekstual. Di sisi lain, kesenjangan prosedural termanifestasi dalam lemahnya mekanisme pengumpulan bukti elektronik, lambatnya akses terhadap data lintas batas, serta ketiadaan kewenangan hukum yang jelas bagi aparat dalam melakukan penyadapan digital atau akses ke konten terenkripsi, yang pada gilirannya menghambat efektivitas penyelidikan dan penuntutan. Kondisi ini diperparah oleh rendahnya kapasitas teknis dan sumber daya manusia di berbagai lembaga penegak hukum, serta fragmentasi koordinasi antarlembaga yang mengakibatkan respons terhadap ancaman siber menjadi terlambat, tidak terintegrasi, dan sering kali tidak komprehensif. Dengan demikian, interaksi antara variabel hukum, institusi, dan teknologi menunjukkan bahwa kekuatan normatif

peraturan tidak akan berarti tanpa dukungan kapasitas operasional dan kerangka koordinasi yang efektif, sebaliknya, kapasitas teknis yang tinggi pun akan sia-sia jika tidak didukung oleh dasar hukum yang memadai dan adaptif.

Implikasi dari temuan ini adalah bahwa penanggulangan terorisme siber di Indonesia tidak dapat lagi didekati secara parsial atau sektoral, melainkan memerlukan pendekatan holistik yang menyatukan perbaikan hukum, penguatan kelembagaan, dan inovasi teknologi dalam satu strategi nasional yang terpadu. Oleh karena itu, untuk menjawab pertanyaan penelitian mengenai kesenjangan hukum dan efektivitas institusi, dapat disimpulkan bahwa kerangka hukum nasional saat ini belum cukup memadai untuk menangani ancaman terorisme siber secara efektif, dan efisiensi penegakan hukum tetap terkendala oleh keterbatasan kapasitas teknis serta koordinasi antarlembaga yang belum optimal, sehingga tanpa transformasi mendasar dalam kedua aspek tersebut, upaya pencegahan dan penindakan terorisme di era digital akan terus menghadapi tantangan struktural yang berpotensi mengancam stabilitas keamanan nasional.

5. DAFTAR PUSTAKA

Ambarita, Folman P. "Penanggulangan Tindak Pidana Terorisme." *Binamulia Hukum* 7, no. 2 (2018): 151.

Durhan, Ainun Sakinah. "Pengaruh Terpaan Informasi Kasus UU ITE Terhadap Kebebasan Berekspresi Pengguna Media Sosial di Kota Makassar." Tesis, Universitas Hasanuddin, 2021.

Enggartyasto, Danang, dan Irwan Hafid. "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia." *Lex Renaissance* 1, no. 7 (2022): 89.

Irviana, Claudia Nuke, dan Roy Valiant Salomo. "Analisis Pengembangan Kapasitas Organisasi Di Direktorat Tindak Pidana Siber (DITTIPIDSIBER), Badan Reserse Kriminal Polri (BARESKRIM POLRI)." *Media Bina Ilmiah* 15, no. 11 (2021): 5690.

Mukti, Aloysius Harry, dan Yohanes Febrian. "Kesiapan Mendeteksi Kegiatan Pendanaan Terorisme Dalam Era Digital Keuangan (Fintech)." *Hukum Pidana dan Pembangunan HUkum* 1, no. 1 (2018): 4.

Nasution, Aulia Rosa. "Penegakan Hukum Terhadap Tindakan Terorisme sebagai 'Extraordinary Crime' dalam Perspektif Hukum Internasional dan Nasional." *LWSA Conference Series* 1 (2018): 8.

Rahmawati, Mety. "Perbandingan Pengaturan Perlindungan Hukum Bagi Penyidik, Penuntut Umum, Hakim, Advokat, Pelapor, Ahli, Saksi Dan Petugas Pemasyakatan Beserta Keluarganya Dalam Perkara Terorisme Indonesia Dan Amerika Serikat." *Hukum Pidana dan Pembangunan HUkum* 1, no. 1 (2018): 2.

Ramdhani, Ahmad Thoriq Akhsan, dan Agung Rashif Madani. "Aktivitas Gen-Z Terhadap Pengembangan UMKM Melalui Digitalisasi (Studi Kasus di Wilayah Kapanewon Moyudan)." *Aplikasia: Jurnal Aplikasi Ilmu-Ilmu Agama* 23, no. 2 (2023): 162.

Riasnugrahani, Missiliana, dan Priska Analya. *Metode Penelitian Kualitatif*. Ideas Publishing, 2023.

Riyono, Tio. "Perkembangan Terorisme dan Anggaran Penanganan

Terorisme di Indonesia." *Buletin APBN* 7, no. 2 (2022): 7.

Saragih, Geofani Milthree. *Metode Penelitian Hukum*. Sada Kurnia Pustaka, 2023.

Sholihin, Ahmad, dan Heri Kurnia. "Internet Sebagai Media Peneybaran Ideologi Radikal: Dampak, Tantangan, dan Upaya Penanggulangannya." *Academy of Social Science and Global Citizenship Journal* 3, no. 1 (2023): 26.

Sukoco, Agung, Muhamad Syauqilah, dan Asep Usman Ismail. "Media, Globalisasi dan Ancaman Terorisme." *Journal of Terrorism Studies* 3, no. 2 (2021): 2.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2024).

Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang (2018).