



Pertanggungjawaban Pidana Pelaku Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional

Gefbi Nopitasari¹; Riska Andi Fitriono²

Fakultas Hukum, Universitas Sebelas Maret, Indonesia

Corresponding author: gefbinopitasari@gmail.com¹

Abstract: The creation of the internet, which is used to make human life easier, has become a new problem because it has given rise to cyber crime in cyberspace. One of the cyber crimes currently developing is cyber terrorism. This research examines the crime of cyber terrorism from the perspective of the perpetrator's criminal responsibility according to national laws in Indonesia. The method used in this research is a normative juridical legal research method that is perspective based on literature study. The legal materials used are primary and secondary legal materials. Data analysis techniques using deductive logical reasoning. The research results show that the term cyber terrorism crime has not been mentioned grammatically in national legislation. However, several articles in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions contain the substance of cyber terrorism crimes, namely Article 28 paragraph (2), Article 28 paragraph (3), Article 31 and Article 33. The legal subject, namely the perpetrator in this article, is "Person" which means an individual or legal entity/corporation. All of these articles contain elements of "acts against the law" whose substance corresponds to the crime of cyber terrorism. So that a person or legal entity that commits acts in accordance with this article can be held criminally responsible. The legal sanction for this crime is imprisonment and/or a fine.

Keywords: Cyber Terrorism, Criminal Liability, National Law

Abstrak: Penciptaan internet yang digunakan untuk kemudahan hidup manusia menjadi problematika baru karena memunculkan kejahatan siber di dunia maya (cyber space). Salah satu kejahatan siber yang berkembang saat ini adalah terorisme siber atau cyber terrorism. Penelitian ini mengkaji kejahatan cyber terrorism dari sisi pertanggungjawaban pidana pelaku menurut undang-undang nasional di Indonesia. Metode yang digunakan dalam penelitian ini adalah metode penelitian hukum yuridis normatif yang bersifat perspektif dengan studi kepustakaan. Bahan hukum yang digunakan adalah bahan hukum primer dan sekunder. Teknik analisis data dengan penalaran logika deduktif. Hasil penelitian menunjukkan bahwa istilah kejahatan cyber terrorism belum disebutkan secara gramatikal dalam peraturan perundang-undangan nasional. Namun, beberapa pasal dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mengandung substansi kejahatan cyber terrorism, yaitu Pasal 28 ayat (2), Pasal 28 ayat (3), Pasal 31 dan Pasal 33. Subjek hukum yaitu pelaku dalam pasal tersebut adalah "Orang" yang berarti orang perorangan atau badan hukum/korporasi. Semua pasal tersebut terdapat unsur "perbuatan melawan hukum" yang substansinya sesuai dengan kejahatan cyber terrorism. Sehingga seseorang atau badan hukum yang melakukan perbuatan sesuai pasal tersebut dapat dimintai pertanggungjawaban secara pidana. Sanksi hukum atas kejahatan tersebut adalah pidana penjara dan/atau pidana denda.

Kata kunci: Cyber Terrorism, Pertanggungjawaban Pidana, Undang-Undang Nasional

1. LATAR BELAKANG

Seiring perkembangan zaman modern, inovasi teknologi mengalami kemajuan yang pesat. Internet merupakan hasil dari inovasi teknologi yang tidak dapat lepas dari kehidupan manusia saat ini. Awalnya penciptaan internet digunakan oleh kalangan penguasa seperti militer, namun saat ini digunakan oleh semua kalangan bahkan oleh penjahat (Agus Raharjo, 2002: 3). Dengan adanya internet, dunia menjadi tidak terbatas oleh ruang dan waktu. Banyak aktivitas sehari-hari dan pekerjaan yang tidak hanya dilakukan secara konvensional namun

sekarang dapat dilakukan secara daring (*online*) di dunia maya melalui sistem elektronik. Begitu pula dengan akses informasi yang semakin mudah diakses dan cepat. Dibalik kemudahan adanya internet, ancaman kejahatan terhadap aktivitas di dunia maya turut muncul. Serangan terhadap sistem elektronik atau komputer dengan berbagai motif marak terjadi. Termasuk kejahatan terorisme, saat ini telah berkembang menjadi terorisme siber yang sebelumnya masih dilakukan secara konvensional. Terorisme merupakan kejahatan yang menggunakan kekerasan atau ancaman untuk menakuti dan menimbulkan suasana teror di masyarakat sehingga dapat menimbulkan kerusakan, gangguan keamanan, dan/atau kerugian materiil maupun immateriil dengan motif politik atau ideologi tertentu.

Terorisme siber atau *cyber terrorism* menggunakan internet sebagai sarana melakukan perbuatan, namun tujuannya sama dengan terorisme konvensional. Bentuk-bentuk terorisme siber antara lain serangan terhadap sistem elektronik atau komputer, informasi elektronik, dan/atau data elektronik, penyebaran propaganda bermotif politik atau ideologi tertentu, maupun perbuatan mengancam atau menakuti secara masal yang menimbulkan gangguan keamanan dan suasana damai di masyarakat. Terorisme siber atau *cyber terrorism* merupakan kejahatan jenis baru. Pelaku dalam kejahatan ini dapat perorangan maupun berkelompok/korporasi/badan hukum. Rumusan delik dalam konstruksi pasal undang-undang tentunya harus dapat mengakomodir kejahatan tersebut agar dapat dipertanggungjawabkan secara pidana. Sesuai asas legalitas dalam hukum pidana yaitu "*nullum delictum nulla poena sine praevia lege*" yang berarti bahwa suatu perbuatan tidak dapat dipidana apabila sebelumnya tidak diatur dalam peraturan hukum. Sehingga hal tersebut menciptakan kepastian hukum. Sebab kekosongan hukum berakibat pada terhapusnya pertanggungjawaban suatu kejahatan. Oleh karena itu, penelitian ini mengkaji mengenai pertanggungjawaban pidana pelaku kejahatan *cyber terrorism* menurut undang-undang nasional yang berlaku di Indonesia. Berdasarkan latar belakang yang telah penulis uraikan, maka penelitian ini mengkaji lebih dalam mengenai bagaimana pertanggungjawaban pidana pelaku kejahatan *cyber terrorism* dalam undang-undang nasional yang berlaku di Indonesia.

2. KAJIAN TEORITIS

a. Tinjauan Umum Pertanggungjawaban Pidana

Dalam *cambridge dictionary*, pertanggungjawaban pidana disebut dengan *criminal liability* yang berarti tanggung jawab atas perilaku ilegal apa pun yang menyebabkan kerusakan atau bahaya pada seseorang atau sesuatu. Pertanggungjawaban pidana didasarkan pada adanya kesalahan. Kesalahan dibagi menjadi dua, yaitu *culpa* atau lalai

dan *opzet* atau sengaja yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan atau peraturan perundang-undangan. Kesalahan dibuktikan atas terpenuhinya unsur-unsur tindak pidana sehingga pemidanaan merupakan bentuk pertanggungjawaban (H.M Rasyid Ariman dan Fahmi Raghieb, 2015: 205). Dengan demikian, pertanggungjawaban pidana bertujuan menentukan apakah seseorang terdakwa dipertanggung jawabkan atas suatu tindakan yang termasuk ke dalam tindak pidana atau bukan. Namun seseorang terdakwa dapat menghilangkan pertanggungjawabannya apabila ditemukan suatu unsur yang menyebabkan hilangnya kemampuan bertanggungjawab pada dirinya.

Pertanggungjawaban pidana mengandung asas-asas, unsur, dan teori hukum. Dalam konteks ini adalah asas hukum *nullum delictum nulla poena sine pravia lege* atau disebut dengan asas legalitas. Asas ini berarti bahwa seseorang hanya dapat dijatuhi pidana apabila telah terbukti kesalahannya sebagai tindak pidana yang telah diatur dalam KUHP dan atau peraturan perundang-undangan lain. Asas legalitas, diatur didalam Pasal 1 ayat (1) KUHP, yaitu: “Tiada suatu perbuatan yang dapat dipidana kecuali atas ketentuan perundang-undangan yang telah ada, sebelum perbuatan dilakukan”. Sehingga asas ini menjamin kepastian hukum karena seseorang tidak dapat dimintakan pertanggungjawabannya apabila perbuatan yang dilakukannya belum diatur dalam sebuah peraturan perundang-undangan sebagai tindak pidana. Menurut Sudarto, unsur-unsur pertanggungjawaban pidana yaitu : adanya suatu tindak pidana yang dilakukan oleh pembuat, adanya kesalahan berupa kesengajaan atau kelalaian yang diatur dalam KUHP dan atau peraturan perundang-undangan lainnya, tidak ada alasan pembenar dan pemaaf, adanya pelaku yang memenuhi syarat kemampuan bertanggungjawab yang berarti kondisi batin normal dan berakal sehat.

Menurut Moeljatno, kemampuan bertanggungjawab yaitu:

- 1) Kemampuan untuk membedakan antara perbuatan yang baik dan yang buruk, yang sesuai hukum dan melawan hukum.
- 2) Kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tadi, yang pertama merupakan faktor akal (*Intellectual Factor*) yaitu membedakan antara perbuatan yang diperbolehkan atau tidak, sedang yang kedua merupakan faktor perasaan atau kehendak (*volitional factor*) yaitu dapat menyesuaikan tingkah lakunya dengan apa yang diperbolehkan dan tidak, sebagai konsekuensinya, maka tentunya orang yang tidak mampu menentukan kehendaknya menurut keinsyafannya tentang baik dan buruknya perbuatan tadi maka dia tidak mempunyai kesalahan.

b. Tinjauan Umum Tentang Pelaku

Pelaku adalah orang yang melakukan kejahatan. Menurut Pasal 55 Kitab Undang-Undang Hukum Pidana, pelaku disebut sebagai *pleger* adalah seseorang yang melakukan perbuatan sesuai dengan delik yang dirumuskan dalam peraturan perundang-undangan. Namun, selain pelaku atau *pleger* seseorang dapat dipidana karena terkait dengan tindak pidana yang terjadi. Dalam Kitab Undang-Undang Hukum Pidana dikategorikan menjadi lima, yaitu: orang yang menyuruh melakukan atau *doenpleger*; orang yang turut serta melakukan atau *medepleger*, orang yang menganjurkan atau *uitlokker* (Pasal 55), orang yang sengaja memberi bantuan ketika kejahatan dilakukan, orang yang memberi kesempatan, alat, sarana atau keterangan untuk melakukan kejahatan (Pasal 56).

Menurut Barda Nawawi Arif, Pelaku adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan atau suatu tidak kesengajaan seperti yang diisyaratkan oleh Undang-undang telah menimbulkan suatu akibat yang tidak dikehendaki oleh Undang-undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur objektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau tidak karena gerakan oleh pihak ketiga.

c. Tinjauan Umum Tentang Tindak Pidana

Dalam hukum pidana Belanda, tindak pidana dikenal dengan istilah “*strafbaar feit*”. “*Straf*” berarti pidana atau hukum dan “*baar*” diartikan sebagai dapat atau boleh, serta “*feit*” diartikan sebagai peristiwa, pelanggaran dan perbuatan. Menurut Moeljatno, unsur tindak pidana adalah :

- 1) Perbuatan;
- 2) Yang dilarang (oleh aturan hukum);
- 3) Ancaman pidana (bagi yang melanggar larangan).

Sedangkan menurut Adami Chazawi, dalam Kitab Undang-Undang Hukum Pidana, terdapat beberapa unsur tindak pidana, yaitu unsur tingkah laku, unsur melawan hukum, unsur kesalahan, unsur akibat konstitutif, unsur keadaan yang menyertai, unsur syarat tambahan untuk dapatnya dituntut pidana, unsur syarat tambahan untuk memperberat pidana, unsur syarat tambahan untuk dapatnya dipidana, unsur objek hukum tindak pidana, unsur kualitas subjek hukum tindak pidana, unsur syarat tambahan untuk memperingan pidana

d. Tinjauan Umum Tentang Terorisme

Dalam *Europeas Convention on the Supression on Terrorism* (ECST) di Eropa pada tahun 1977, terorisme dirumuskan sebagai perluasan paradigma arti dari *Crimes against State* menjadi *Crime Against Humanity*. Paradigma tersebut berubah menjadi tindak Pidana untuk menciptakan suatu keadaan yang mengakibatkan individu, golongan dan masyarakat umum ada dalam suasana yang teror. Istilah “*terorisme*” secara etimologi berasal dari kata “*teror*” dalam bahasa Latin “*terrere*” atau dalam bahasa Inggris “*to fright*” yang diterjemahkan dalam bahasa Indonesia berarti “menakutkan” atau “mengerikan” (Mardenis, 2013: 85). Terorisme memiliki konotasi yang sangat sensitif karena terorisme menyebabkan terjadinya pembunuhan dan kesengsaraan. Perbedaan pandangan tentang terorisme tergantung dari sisimana memandangnya dan siapa yang memandang (Mardenis, 2013: 86-87).

Terorisme menurut Pasal 1 ayat 2 Undang-Undang Nomor 15 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 adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan. Sedangkan pada Pasal 1 ayat 1, Tindak Pidana Terorisme adalah segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Undang-Undang tersebut. Menurut Pasal 5 Undang-Undang Nomor 15 Tahun 2018, tindak pidana terorisme yang diatur dalam Undang-Undang tersebut harus dianggap bukan tindak pidana politik, dan dapat diekstradisi atau dimintakan bantuan timbal balik sebagaimana diatur dalam ketentuan peraturan perundang-undangan.

e. Tinjauan Umum Tentang Dunia Maya (*Cyberspace*)

Cyberspace atau dunia maya adalah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara online (terhubung langsung). Dunia maya ini merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan komputer (sensor, transduser, koneksi, transmisi, prosesor, signal, pengontrol) yang dapat menghubungkan peralatan komunikasi (komputer, telepon genggam, instrumentasi elektronik, dan lain-lain) yang tersebar di

seluruh penjuru dunia secara interaktif. Kejahatan dunia maya adalah kejahatan yang dilakukan di *Cyberspace* menggunakan komputer dan teknologi jaringan yang disediakan oleh infrastruktur Informasi dan Komunikasi. Chawki, (2009) Tren yang dapat diamati telah menunjukkan bahwa penegakan hukum belum dapat meningkatkan dalam memenuhi tantangan baru yang ditimbulkan oleh *Cybercrime* terhadap kesejahteraan berbagai kategori pengguna di Internet (Brenner, 2007).

f. Tinjauan Umum Tentang *Cyber Terrorism*

Cyber Terrorism berasal dari kata bahasa Inggris yaitu “*cyber*” yang berarti dunia maya dan “*terrorism*” yang berarti terorisme. *Cyber Terrorism* merupakan jenis terorisme yang menggunakan jaringan internet dan komputer/sistem elektronik. Definisi menurut beberapa ahli dan literatur sebagai berikut:

- 1) James A. Lewis mendefinisikan *Cyber Terrorism* sebagai Penggunaan jaringan komputer sebagai sarana untuk melumpuhkan insfrastruktur secara nasional, seperti energy, transportasi, untuk menekan/mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil “*The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government population)*”.
- 2) Menurut Dorothy E. Denning, *cyber terrorism* sebagai “Penyerangan dengan menggunakan komputer atau mengancam, mengintimidasi atau memaksa pemerintahan atau masyarakat, dengan tujuan untuk mencapai target politik, agama atau ideology. Sarana itu cukup untuk menimbulkan rasa takut yang berasal dari tindakan psikis teroris. Serangan itu secara tidak langsung dapat menimbulkan kerugian fisik atau materil.
- 3) Dalam *Encyclopedia of Cybercrime* kejahatan *Cybercrime* dibagi ke dalam beberapa jenis dan salah satunya adalah *Cyber terrorism*. *Cyber terrorism* adalah kejahatan yang dilakukan oleh oknum yang bermaksud mengedepankan tujuan sosial, agama atau politik namun dengan cara menyebabkan rasa takut yang meluas atau dengan merusak atau mengganggu informasi infrastruktur yang penting. (McQuade, 2009:44) Berdasarkan penjelasan jenis-jenis *Cybercrime*, *Cyber terrorism* merupakan kejahatan yang baru muncul. Kejahatan ini menggunakan media komputer dalam menyebarkan ideologi yang bersifat terror guna menjalankan aksi kejahatan teroris di internet (Astuti, 2015:165).

Secara garis besar, *cyber terrorism* dapat dibagi menjadi dua bentuk atau karakteristik, yaitu sebagai berikut (M. Habibie Ginting, 2016):

- 1) *Cyber terrorism* yang memiliki karakteristik sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan informasi yang tersimpan didalam komputer;
- 2) *Cyber terrorism* berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media teror kepada pemerintah dan masyarakat.

Penyebab *cyber terrorism* menurut Zhang ada lima, yaitu (M. Habibie Ginting, 2016):

- 1) *Psychological Warfare*. Menurut Zhang, “*The study of the modern terrorism also reveals one of the most important characteristics of the terrorism is to raise fear.*” Motif ini tidak berbeda dengan motif terorisme konvensional, dimana sasaran utama terorisme adalah menimbulkan rasa ketakutan dalam masyarakat;
- 2) *Propaganda*. Melalui *cyber terrorism*, kelompok teroris dapat melakukan propaganda tanpa banyak hambatan seperti sensor informasi, karena sifat Internet yang terbuka, upaya ini jauh lebih efektif;
- 3) *Fundraising*. Melalui *cyber terrorism*, khususnya tindakan penyadapan dan pengambilalihan harta pihak lain untuk kepentingan organisasi teroris telah menjadi motif utama dari *cyber terrorism*. Kelompok teroris juga dapat menambah keuangannya melalui penjualan CD dan buku tentang “perjuangan” mereka;
- 4) *Communication*. Motif selanjutnya dari *cyber terrorism* adalah komunikasi. Kelompok teroris telah secara aktif memanfaatkan Internet sebagai media komunikasi yang efektif dan jauh lebih aman dibandingkan komunikasi konvensional;
- 5) *Information Gathering*. Kelompok teroris memiliki kepentingan terhadap pengumpulan informasi untuk keperluan teror, seperti informasi mengenai sasaran teror, informasi kekuatan pihak musuh, dan informasi lain yang dapat menunjang kinerja kelompok teroris tersebut seperti informasi rahasia (*intelligent information*) terkait persenjataan, dan lainnya. Atas dasar motif *information gathering* kejahatan tersebut dilakukan.

Singkatnya, *cyber terrorism* adalah kejahatan yang bertujuan menimbulkan teror atau menyebar propaganda pendukung kejahatan teror melalui sarana internet yang dapat menyebabkan kerugian materil dan atau immateril dengan motif ideologi politik tertentu. Penelitian terdahulu yang menunjang penelitian ini sebagai berikut :

- 1) Skripsi oleh Adnan Brilian Ulapia mahasiswa Universitas Sriwijaya pada tahun 2020 dengan judul “*Perspektif Hukum Pidana Indonesia Terhadap Cyber Terrorism*”. Penelitian ini mengkaji pengaturan tindak pidana cyber terrorism secara luas dan tidak menggunakan putusan kasus tertentu sebagai bahan hukum penelitian.

- 2) Skripsi oleh Oki Putri Amdini mahasiswa Universitas Negeri Semarang pada tahun 2020 dengan judul “Tinjauan Yuridis Tindak Pidana *Cyber Terrorism* Dalam Perspektif Kejahatan Transnasional Terorganisir”. Penelitian ini menguraikan modus operandi dan pengaturan tindak pidana *Cyber terrorism* dengan perpektif kejahatan transnasional terorganisir. Penelitian ini mengkaji instrumen hukum internasional tanpa mengkaji peraturan nasional yang terkait meski di tempat kejahatan tersebut terjadi.

3. METODE PENELITIAN

Penelitian ini adalah jenis penelitian hukum doktrinal atau disebut juga sebagai penelitian hukum normatif. Menurut Peter Mahmud Marzuki, penelitian hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi (Marzuki P. Mahmud, 2010: 35). Penelitian hukum doktrinal adalah penelitian yang mengkaji data sekunder. Penelitian hukum doktrinal atau normatif sering disebut juga sebagai penelitian hukum kepustakaan karena peneliti meneliti bahan pustaka. Sehingga, penelitian ini mendasarkan analisis pada peraturan perundang-undangan yang berlaku terkait permasalahan yang akan dikaji. Penelitian ini bersifat preskriptif yang berarti bahwa penelitian hukum mempelajari penerapan konsep, prinsip, aturan, maupun tujuan norma hukum yang telah ada terhadap permasalahan yang diteliti. Penulisan hukum memberikan petunjuk yang didasarkan pada ketentuan resmi dan/atau ketentuan yang tengah berlaku (Ulum, 2022). Pendekatan yang digunakan adalah pendekatan undang-undang (*statute approach*) guna memecahkan permasalahan. Penelitian ini menggunakan bahan hukum primer dan sekunder. Bahan hukum primer meliputi peraturan perundang-undangan dan segala dokumen resmi yang memuat ketentuan hukum. Berikut bahan hukum primer yang penulis gunakan dalam penelitian ini:

- a. Kitab Undang-Undang Hukum Pidana.
- b. Undang-Undang 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.
- c. Undang-Undang Nomor 1 Tahun 2004 Tentang Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
- d. Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme.

Bahan hukum sekunder yang digunakan untuk menunjang penelitian ini adalah penelitian terdahulu berupa skripsi yang berkaitan dengan isu hukum penelitian ini dan artikel ilmiah yang terbit pada jurnal yang kredibel terkait isu hukum penelitian ini. Teknik pengumpulan data pada penelitian ini berupa studi kepustakaan dengan metode *library research*. Penulis melakukan pengumpulan data dengan cara penelusuran untuk mencari bahan-bahan hukum yang telah disebutkan sebelumnya yaitu dengan membaca dan menelaah berbagai literatur yang bersumber dari bahan hukum primer dan sekunder. Teknik analisis data dilakukan dengan metode silogisme dan interpretasi. Penelitian ini menggunakan logika deduktif yaitu menarik kesimpulan secara khusus dari penjelasan suatu hal yang bersifat umum. Isu hukum penelitian ini dikaitkan dengan penafsiran peraturan perundang-undangan terkait.

4. HASIL DAN PEMBAHASAN

Pertanggungjawaban pidana merupakan suatu bentuk pertanggungjawaban seseorang atau badan hukum terhadap perbuatan yang dilakukan dalam koridor hukum pidana dengan menerima sanksi hukuman. Pertanggungjawaban atas suatu tindak pidana didasarkan pada asas legalitas yang dikenal dengan *nullum delictum nulla poena sine praevia lege* berdasarkan pasal 1 ayat (1) KUHP yang berbunyi “Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan ketentuan perundang-undangan yang telah ada”. Subjek pelaku dalam tindak pidana dapat dibedakan menjadi dua, yaitu orang (*naturlijk person*) dan badan hukum atau korporasi (*recht person*). Tindak pidana terorisme yang secara khusus bergerak dalam dunia maya (*cyberspace*) yang disebut dengan terorisme siber atau *cyber terrorism* belum diatur secara terang dan jelas (*expressive verbis*) dalam undang-undang nasional. Hal tersebut membuat pertanggungjawaban pidananya menjadi rancu karena tindak pidana tersebut merupakan gabungan antara *cyber crime* dan terorisme. Dalam perkara tindak pidana terorisme secara umum pelaku dapat mencakup orang (*naturlijk person*) dan atau korporasi (*recht person*). Secara khusus dalam tindak pidana *cyber terrorism* melalui media sosial, perlu adanya batasan yang jelas terhadap pemilik akun media sosial maupun pemilik platform digital elektronik mengingat kejahatan terorisme ini dilakukan di dunia maya (*cyber space*). Pengaturan terhadap subjek pelaku tindak pidana terorisme maupun pelaku *cyber crime* terkandung dalam beberapa undang-undang, yaitu :

- a. Pasal 1 ayat 3 Undang-Undang Nomor 9 Tahun 2013 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme yang berbunyi :

“Setiap orang adalah orang perseorangan atau korporasi.”

- b. Pasal 1 ayat 9 Undang-Undang 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 yang berbunyi :

“Setiap orang adalah orang perseorangan atau korporasi.”

- c. Pasal 1 ayat (10) Undang-Undang 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 yang berbunyi :

“Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi, baik merupakan badan hukum maupun bukan badan hukum.”

- d. Pasal 1 ayat (21) dan Pasal 1 ayat (22) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, turut mengatur subjek pelaku tindak pidana pada dunia maya (*cyber crime*) yang berbunyi :

“21. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.”

“22. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.”

Peraturan di bidang *cyber* dan peraturan di bidang terorisme dikelompokkan dalam peraturan perundang-undangan yang berbeda. *Cyber terrorism* merupakan bagian dari bentuk kejahatan *cyber crime*, sesuai dengan pendapat Denning (2000), *cyber terrorism* merupakan konvergensi dari *cyberspace* dan terorisme. Oleh karena itu, karakteristik terorisme dalam *cyber terrorism* berbeda dengan tindak pidana terorisme secara umum. Karakteristik *cyber terrorism* bukan hanya tentang menggunakan unsur media telekomunikasi dan informasi yang digunakan sebagai sarana dan objek sasaran untuk melaksanakan aksi terorisme. Namun, lebih dikedepankan kepada penggunaan internet di dunia maya (*cyber space*) untuk melakukan tindakan atau serangan terhadap sistem elektronik termasuk penyebaran, intersepsi, peretasan informasi dan/atau dokumen elektronik yang dapat mengakibatkan provokasi, kebencian, ketakutan, dan ancaman kerusakan di tengah masyarakat dengan tujuan politik tertentu. Khususnya *cyber terrorism* melalui media sosial yang digunakan untuk membuat provokasi dan kebencian yang disebarkan melalui platform digital sosial seperti telegram, instagram, facebook, twitter, dan sebagainya. Hal ini disebabkan fungsi media sosial yang merupakan alat untuk berkomunikasi, berekspresi, dan berinovasi dalam

wadah digital elektronik yang mudah diakses oleh masyarakat. Sehingga dengan penggunaan media sosial sasaran atau target dapat dijangkau dengan mudah dan luas.

Penerapan undang-undang untuk menjerat tersangka tindak pidana *cyber terrorism* melalui media sosial menjadi rancu karena bersinggungan antara bidang terorisme dengan bidang telekomunikasi dan informasi. Peraturan hukum yang mengatur mengenai tindak pidana *cyber terrorism* di Indonesia sampai saat ini belum jelas dan pasti (Agis Josianto Adam 2014:165). Kitab Undang-Undang Hukum Pidana dan Undang-Undang tentang Pemberantasan Tindak Pidana Terorisme tidak mengandung definisi secara gramatikal mengenai *cyber terrorism*. Namun, sesuai yuridiksi Undang-Undang tentang Informasi dan Transaksi Elektronik yaitu dunia maya (*cyber space*) dan sebagai induk peraturan *cyber crime* termasuk aktivitas media sosial, maka beberapa pasal yang muatannya mengandung esensi *cyber terrorism* dalam Undang-Undang tentang Informasi dan Transaksi Elektronik lebih tepat digunakan. Berikut ini pengaturan *cyber terrorism* dalam beberapa undang-undang :

1) Pengaturan *Cyber Terrorism* di dalam Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan induk peraturan hukum pidana Indonesia. Namun, kaitannya dengan *cyber terrorism*, KUHP tidak lengkap dan tidak dapat mengakomodir masalah hukum ini karena berdimensi tindak pidana baru. Di dalam Kitab Undang-Undang Hukum Pidana (KUHP) *cyber terrorism* tidak disebutkan secara gramatikal. KUHP masih bersifat konvensional sehingga tidak memenuhi kualifikasi kejahatan tindak pidana *cyber terrorism* yang dilakukan di dunia maya. Pasal yang mendekati namun tidak dapat diterapkan antara lain tentang kejahatan terhadap ketertiban umum pada pasal 168 ayat (3) tentang mengeluarkan ancaman atau menakut-nakuti orang yang berbunyi :

“Bila ia mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, maka ia diancam dengan pidana penjara paling lama satu tahun empat bulan.”

Ayat tersebut masih berhubungan dengan dua ayat sebelumnya tentang pemaksaan memasuki sebuah duniaan dengan perusakan, namun rumusan tindak pidananya konvensional dan tidak memuat motif ideologi politik meskipun narasinya menggunakan ancaman yang mengganggu ketertiban umum. Sehingga ketika dikolerasikan dengan kejahatan *cyber terrorism* melalui media sosial, maka pasal 168 ayat (3) Kitab Undang-Undang Hukum Pidana (KUHP) tersebut tidak dapat digunakan untuk menjerat seseorang/badan hukum sebagai pelaku tindak pidana. Oleh karena itu, tidak ada pertanggungjawaban pidana bagi pelaku kejahatan *cyber terrorism* di dalam KUHP.

- 2) Pengaturan *Cyber Terrorism* di dalam Undang-Undang 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.

Undang-Undang tersebut mengatur tentang tindak pidana terorisme secara umum. Tindak pidana terorisme adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan. Perkembangan teknologi saat ini membuat kejahatan terorisme turut berkembang di dalam dunia maya yang disebut sebagai *cyber terrorism*. Di dalam undang-undang ini, kejahatan *cyber terrorism* yang pada dasarnya terjadi pada dunia maya (*cyber space*) tidak disebutkan dengan jelas maupun didefinisikan secara gramatikal. Berikut ini pasal yang mendekati bentuk kejahatan *cyber terrorism*, yaitu Pasal 6 Undang-Undang Terorisme yang berbunyi:

“Setiap Orang yang dengan sengaja menggunakan Kekerasan atau Ancaman Kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas, menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap Objek Vital yang Strategis, lingkungan hidup atau Fasilitas Publik atau fasilitas internasional dipidana dengan pidana penjara paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun, pidana penjara seumur hidup, atau pidana mati”.

Berdasarkan isi pasal di atas, pasal tersebut dapat ditafsirkan mendekati dengan bentuk kejahatan *cyber terrorism*. Terletak pada frasa ancaman kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas serta menimbulkan korban yang bersifat masal. Sehingga terdapat ancaman bahaya untuk menimbulkan rasa takut. Unsur-unsur yang terdapat dalam terorisme konvensional, yakni: adanya kerusakan, ketidakpastian, ketakutan, keputusasaan bahkan kematian. Tindak pidana *cyber-terrorism* harus dilihat terlebih dahulu identitas pelaku, motivasi, dan tujuan yang dilakukannya, serta akibatnya (Varvara 2001:5). Serangan *cyber-terrorism* tetap terdiri dari unsur-unsur yang terdapat dalam terorisme konvensional (Janet, dkk 2004:280). Namun, celah dari Pasal 6 Undang-Undang Terorisme ini adalah bahwa dalam rumusannya tidak disebutkan perihal instrumen apa yang digunakan oleh pelaku teror

dalam melakukan aksinya, sedangkan tindak pidana *cyber terrorism* ini menggunakan sarana jaringan internet untuk melaksanakan kegiatannya. Modus dan bentuk kejahatan terorisme siber terus mengalami progres perkembangan yang signifikan. Pasal 6 tersebut berlaku bagi pelaku “orang” atau individu dan tidak menjerat badan hukum atau korporasi. Sanksi pidana terhadap pelaku tindak pidana dalam pasal tersebut, yaitu pidana penjara dengan waktu paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun, pidana penjara seumur hidup, atau pidana mati.

3) Pengaturan *Cyber Terrorism* di dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Informasi Dan Transaksi Elektronik (ITE) merupakan payung hukum peraturan aktivitas elektronik. Aktivitas elektronik merupakan segala tindakan yang terjadi di dunia maya dengan media jaringan internet. Dengan adanya undang-undang ini, berbagai jenis tindak pidana yang telah berkembang akibat kemajuan IPTEK dapat terakomodir. Salah satunya adalah tindak pidana terorisme siber (*cyber terrorism*). Dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) terdapat beberapa pasal yang dapat dikaitkan dan ditafsirkan dengan kejahatan *cyber terrorism* karena substansinya terpenuhi antara lain dilakukan di dunia maya, mengandung kalimat provokasi kebencian atau ideologi, dapat menimbulkan permusuhan atau kedamaian. Sehingga dapat dipertanggungjawabkan secara pidana, meskipun tidak menyebutkan secara eksplisit kalimat terorisme siber (*cyber terrorism*), yaitu :

a) *Pertama*, Pasal 28 ayat (2)

Pasal 28 ayat (2) berbunyi :

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik.”

Pasal tersebut mengandung unsur “setiap orang” yang menunjukkan subjek hukum pelaku tindak pidana, yaitu orang/*persoon*. Menurut Pasal 1 ayat (21) pengertian “Orang” adalah orang perseorangan atau badan hukum/korporasi. Sehingga pasal tersebut digunakan untuk menjerat pelaku secara perorangan maupun sebagai perwakilan badan hukum/korporasi. Sehingga dalam pasal ini badan hukum/korporasi

apabila melakukan kejahatan *cyber terrorism* dapat dimintai pertanggungjawaban secara pidana karena dilimpahkan kepada individu. Pasal ini turut mengandung substansi dalam terorisme yaitu memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan SARA, kepercayaan, agama dan sebagainya. Serta terdapat unsur mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang tentunya terjadi di dunia maya (*cyber space*). Sanksi pidana atas kejahatan menurut pasal tersebut diatur dalam Pasal 45 A yang berbunyi :

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak, atau memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Berdasarkan pasal tersebut, maka sanksi pidana yang dijatuhkan kepada pelaku tindak pidana dalam Pasal 28 ayat (2) sebagai bentuk pertanggungjawabannya adalah pidana penjara dan/atau denda. Pidana penjara dengan waktu paling lama enam tahun sedangkan denda paling banyak sebesar satu miliar rupiah.

b) *Kedua*, Pasal 28 ayat (3)

Pasal 28 ayat (3) berbunyi :

“Setiap Orang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat.”

Pasal tersebut mengandung unsur “setiap orang” yang berarti seseorang sebagai subjek hukum yang bertanggungjawab terhadap suatu perbuatan, disebut sebagai pelaku. Tidak terdapat kalimat korporasi atau badan hukum, namun menurut teori pertanggungjawaban pidana korporasi maka dapat dilimpahkan kepada seseorang atau individu yang melakukan dan menggerakkan aktivitas tersebut. Unsur menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik, tentunya terjadi di dunia maya (*cyber space*) yang merupakan salah satu substansi *cyber terrorism*. Kemudian terdapat unsur “memuat pemberitaan bohong yang menimbulkan kerusuhan”, dapat digunakan untuk menjerat seseorang sebagai pelaku *cyber terrorism* karena informasi yang tidak

dapat divalidasi kebenarannya dapat mengandung provokasi. Sehingga dapat mengganggu perdamaian di masyarakat yang dapat menimbulkan aksi anarkisme atau kerusuhan. Terhadap perbuatan dalam pasal di atas, sanksi hukuman pidananya diatur dalam Pasal 45 A ayat (3) yang berbunyi :

“Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat sebagaimana dimaksud dalam Pasal 28 ayat (3) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Sehingga seseorang secara individu atau korporasi/badan hukum sebagai pelaku dapat dipertanggungjawabkan secara pidana apabila telah memenuhi unsur-unsur dalam pasal tersebut dengan pidana penjara maksimal selama enam tahun dan/atau denda paling banyak sebesar satu miliar rupiah.

c) *Ketiga*, Pasal 31 dan Pasal 33

Ketentuan dalam Pasal 31 yang dihubungkan (*juncto*) dengan Pasal 33 dapat mengakomodir kejahatan *cyber terrorism* intersepsi dan serangan data yang mengakibatkan gangguan sistem elektronik dan ancaman stabilitas keamanan masyarakat. Pasal 31 terdiri dari dua ayat yang berbunyi :

“(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.”

“(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.”

Sedangkan Pasal 33 berbunyi “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

Pasal 31 tersebut mengandung unsur “setiap orang” yang berarti orang perseorangan sebagai subjek hukum yang bertanggungjawab secara individu atau korporasi/badan hukum karena pada Pasal 1 ayat (21) telah dijelaskan pengertian

“orang”. Kemudian terdapat unsur “dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain” yaitu terjadi peristiwa intersepsi atau penyadapan secara sengaja dengan diawali adanya niat dari pelaku terhadap informasi dan/atau dokumen elektronik milik orang lain.

Pasal 33 mengandung unsur “setiap orang” yang berarti orang sebagai individu atau badan hukum merupakan subjek hukum yang disebut sebagai pelaku. Sesuai dengan Pasal 1 ayat (21) bahwa orang adalah orang perseorangan atau badan hukum. Kemudian terdapat unsur “dengan sengaja dan tanpa hak atau melawan hukum” yaitu adanya niat atau sikap batin dari dalam diri orang secara sadar untuk melakukan sesuatu yang dilarang. Serta unsur “melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya” yang menunjukkan bahwa akibat dari tindakan seseorang tersebut adalah terganggunya sistem elektronik sehingga tidak bekerja dengan baik. Dalam rumusan kedua Pasal tersebut terdapat frasa melawan hukum atau *wederrechtelijkheid* yang berarti bahwa seseorang dapat dinyatakan melawan hukum ketika perbuatan yang dilakukan adalah suatu perbuatan yang dilarang oleh hukum (Eddy O.S Hiariej 2016:232). Konstruksi pasal 31 tersebut terdapat unsur objektif yaitu sistem elektronik atau komputer bukan milik pelaku dan tindakan mengakses sistem elektronik atau komputer termasuk informasi/dokumen elektronik tersebut melawan hukum. Unsur subjektif yaitu pelaku secara sengaja memiliki niat jahat untuk mengakses komputer secara illegal. Sedangkan dalam Pasal 33 terletak pada akibat tindakan pelaku yaitu terganggunya sistem elektronik sehingga tidak dapat digunakan dengan baik sesuai dengan fungsinya. Hal tersebut dapat digunakan untuk menjerat pelaku kejahatan *cyber terrorism* yang melakukan intersepsi atau penyadapan data nasional instansi pemerintahan maupun organisasi tertentu yang dapat mengakibatkan gangguan kedamaian dan pelayanan kepada masyarakat. Sanksi hukum atas kejahatan dalam Pasal 31 tersebut diatur pada Pasal 47 yang berbunyi :

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).”

Untuk kejahatan dalam Pasal 33 diatur pada Pasal 49 yang berbunyi :

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).”

Oleh karena itu pertanggungjawaban pidana pelaku kejahatan dalam Pasal 31 jo. Pasal 33 ini dibebankan kepada orang perorangan baik secara individu atau korporasi/badan hukum apabila telah memenuhi unsur-unsur yang telah diuraikan tersebut dengan sanksi pidana penjara maksimal sepuluh tahun dan/atau denda maksimal delapan ratus juta rupiah hingga sepuluh miliar rupiah.

4) Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme

Pendanaan terorisme merupakan perbuatan berupa pengumpulan dana yang bertujuan untuk pembiayaan kegiatan terorisme dan/atau operasional organisasi teroris. Pengertian pendanaan terorisme menurut Pasal 1 angka 1 yang berbunyi:

“Pendanaan Terorisme adalah segala perbuatan dalam rangka menyediakan, mengumpulkan, memberikan, atau meminjamkan Dana, baik langsung maupun tidak langsung, dengan maksud untuk digunakan dan/atau yang diketahui akan digunakan untuk melakukan kegiatan terorisme, organisasi teroris, atau teroris”. Dalam menjalankan perbuatan tersebut, umumnya melalui transaksi keuangan secara manual maupun menggunakan sarana internet. Transaksi menggunakan sarana internet antara lain *internet banking*, *mobile banking* via aplikasi *smartphone*, dan *payment* yang tentunya terjadi di dunia maya (*cyber space*). Namun, dalam undang-undang ini tidak terdapat pasal yang secara spesifik menyebutkan perihal pendanaan terorisme melalui transaksi internet (*online*). Pengaturan terkait hal tersebut terakomodir dalam Undang-Undang ITE pada Pasal 33. Oleh karena itu, Undang-Undang Pendanaan Terorisme tidak dapat diterapkan untuk menjerat seseorang baik secara orang perorangan atau badan hukum/korporasi sebagai pelaku kejahatan *cyber-terrorism*, sehingga tidak ada pertanggungjawaban pidananya dalam undang-undang tersebut.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah diuraikan dalam pembahasan, maka dapat disimpulkan bahwa kejahatan *cyber terrorism* belum diatur secara spesifik dan belum disebutkan secara gramatikal dalam undang-undang nasional yang dikaji. KUHP tidak mengatur perihal kejahatan tersebut karena rumusannya masih bersifat konvensional dan umum. Undang-Undang Terorisme tidak mengatur kejahatan tersebut karena rumusannya

berisi terorisme konvensional, belum mengandung delik terorisme siber yang terjadi di dunia maya. Selanjutnya, dalam Undang-Undang Pendanaan Terorisme belum mengatur perihal *cyber terrorism* meskipun transaksi keuangan saat ini dapat dilakukan secara *online* yang dapat menjadi celah terjadinya kejahatan tersebut. Namun, substansi *cyber terrorism* dan beberapa delik kejahatan tersebut dapat diakomodir dalam Pasal 28 ayat (2), Pasal 28 ayat (3), Pasal 31 dan Pasal 33 Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sesuai dengan yurisdiksi undang-undang tersebut yaitu sebagai payung hukum aktivitas di dunia maya (*cyber space*). Pelaku sebagai subjek hukum kejahatan tersebut yaitu orang perorangan atau badan hukum. Sanksi hukumnya adalah pidana penjara dan/atau pidana denda. Revisi Undang-Undang Informasi dan Transaksi Elektronik(ITE) dan Undang-Undang Terorisme wajib dilakukan pemerintah pusat yaitu Presiden dan parlemen yaitu Dewan Perwakilan Rakyat (DPR) agar dapat mengakomodir kejahatan *cyber terrorism*. Sehingga tidak terjadi kekosongan hukum mengenai kejahatan *cyber-terrorism* dan mewujudkan kepastian, keadilan, dan kemanfaatan hukum.

DAFTAR REFERENSI

- Adam, A.J. (2014). Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik. *Jurnal Lex Administratum*, 2(2), 164-173.
- Aditya, A.R.M., Kertopati, S.N.H., & Prasetyo, T. B. (2023). Potensi Ancaman Terorisme Dalam Penyebaran Penggunaan Ied Melalui Media Sosial. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 10(2), 813-824.
- Afriansyah, A., Khozi, A., & Wargadalem, M.A. (2023). Hukum Dan Kebijakan Indonesia Dalam Memerangi Pendanaan Terorisme: Sebuah Analisa Pemutakhiran. *Aml/Cft Journal Ppatk*, 2(1), 1-8.
- Andini, O.P. (2020). Tinjauan Yuridis Tindak Pidana *Cyber Terrorism* Dalam Perspektif Kejahatan Transnasional Terorganisir. Universitas Negeri Semarang. Retrieved from <http://lib.unnes.ac.id/39108/>
- Argastya, A.Y., & Supanto. (2022). Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber-Terrorism. *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, 11(1), 10-28. <https://doi.org/10.20961/recidive.v11i1.67425>
- Ariman, H.M.R., Raghieb, F. (2015). *Hukum Pidana*. Malang: Setara Press.
- Astuti, S.A. (2015). Penegakan Hukum terhadap Terorisme Dunia Maya di Indonesia. *Rechtsidee*, 2(2), 79-178.

- Blogger. (2011). Pengertian Cyber Terorism. Available at: <http://eptikbsikel9.blogspot.co.id/2015/04/pengertian-cyber-terrorism.html>.
- Cambridge, Org. (2023). Available at: <https://dictionary.cambridge.org/dictionary/english/criminal-liability>.
- Dina, H.A.I. (2021). Aksi Cyber-Terrorism di Amerika Serikat dalam Perspektif Keamanan Global. *Global & Policy*, 9(2), 130-134.
- Hiariej, E.O.S. (2014). *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka
- Jondong, Z. (2020). Kebijakan Hukum Pidana Bagi Tindak Pidana Cyber Terrorism Dalam Rangka Pembentukan Hukum Positif Di Indonesia. *Jurnal Preferensi Hukum*, 1(2), 21-27.
- Lubis, R.R. (2017). Potensi Pengguna Internet Indonesia Dalam Menanggung Radikalisasi Siber. *Jurnal Pertahanan & Bela Negara*, 7 (2), 19-34. <https://doi.org/10.33172/jpbh.v7i2.177>
- Makarim, E. (2021). Cyber Terrorism Prevention And Eradication In Indonesia And Role And Functions Of Media. *Indonesian Journal of International Law*, 7(3), 6. <https://doi.org/10.17304/ijil.vol7.3.236>
- Marzuki, P.M. (2014). *Penelitian Hukum* (Edisi Revisi). Jakarta: PT. Raja Grafindo Persada
- Miftahul, U. (2022). *Modul Metode Penelitian Dan Penulisan Hukum*. Bandung: Penerbit Widiana.
- Moeljatno. (2015). *Azas – Azas Hukum Pidana*. Jakarta: Rineka Cipta, cetakan ke-9.
- Mumtaaz, G. M., Wardhana, T. R., & Diastutui, F. H. (2021). Anti Cyber Terorism Sebagai Upaya Strategis Dalam Menanggulangi Cyber Terorism Di Indonesia. *Al-Hakam Islamic Law & Contemporary Issues*, 2(2), 48-59. Diambil dari ejournal2.undip.ac.id
- Nasution, A. F., Desri, R. S., & Nurbaiti, W. S. (2023). Lingkup Dunia Cyber di Indonesia. *Comserva: (Jurnal Penelitian dan Pengabdian Masyarakat)*, 2(11), 2477-2486. <https://doi.org/10.36418/comserva.v2i11.653>
- Nurita, C. (2024). Penegakan Hukum Terhadap Pelaku Penyebaran Propaganda Tindak Pidana Terorisme Melalui Media Sosial. *Jurnal Ilmiah Metadata*, 6(1), 154-164.
- Peraturan Perundang-Undangan (n.d). Kitab Undang-Undang Hukum Pidana (KUHP)
- Peraturan Perundang-Undangan (n.d). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Peraturan Perundang-Undangan (n.d). Undang-Undang 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.

Peraturan Perundang-Undangan (n.d). Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme Kitab Undang-Undang Hukum Pidana

Perdana, Andre Pebrian., & Yusuf, Winardi. (2020). UU ITE Tentang Efek Media Sosial Terhadap Generasi Milenial. *Jurnal Kelitbangan*, 8(3), 297-308.

Raharjo, A. (2002). *Cyber Crime*. Bandung: Citra Aditya Bakti.

Rozika, W. (2019). “Propaganda Dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrin Naim)”. *Jurnal Ilmu Kepolisian* , 11 (2), 13. <https://doi.org/10.35879/jik.v11i2.89>

Sarinastiti, E.N. (2018). Internet Dan Terorisme: Menguatnya Aksi Cyber-Terrorism Global Melalui Media Baru. *Universitas Gadjah Mada* , 1 (1), 40–52.

Ulapia, Adnan Brilian. (2020). Perspektif Hukum Pidana Indonesia Terhadap *Cyber Terrorism*. Universitas Sriwijaya. Retrieved from <https://repository.unsri.ac.id/35662/>