Jurist-Diction
Volume 7 No. 2, April 2024

Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana

Alfendo Yefta Argastya
alfendoyefta02@gmail.com
Universitas Sebelas Maret

How to cite:
Alfendo Yefta Argastya'Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana' (2024) Vol. 7 No. 2 Jurist-Diction

Histori artikel:
Submit 31 Januari 2024;
Diterima 08 Maret 2024;
Diterbitkan 19 April 2024.

DOI:
10.20473/jd.v7i2.44633

p-ISSN: 2721-8392
e-ISSN: 2655-8297

Abstract

The Article aims to construct a rule of law in order to tackle cyber-terrorism crimes in Indonesia. In essence, changes in technological developments have a positive impact in the framework of increasing human welfare, progress and civilization, but these technological and information developments also have a negative impact. One of them is a crime using computer and internet media known as cybercrime. This study uses normative legal research and statutory, conceptual, and comparative approaches. Whereas the results of the study show that compared to other countries, Indonesia has experienced delays in regulating legal formulations regarding cybercrime, especially cyber-terrorism. In addition, law enforcement is also experiencing ambiguity because there is no instrument that regulates clearly and unequivocally. In this context, Indonesia must use the politics of criminal law to compile and regulate cyber-terrorism crimes in the context of overcoming cybercrimes. Therefore, the government must immediately make regulations or draft laws to anticipate cyber-terrorism crimes.
Keywords: *Cybercrime; Cyber-terrorism; Criminal Law Politics.*

Abstrak

Artikel ini bertujuan untuk mengonstruksi sebuah aturan hukum dalam rangka menanggulangi kejahatan cyber-terrorism di Indonesia. Pada hakikatnya perubahan dalam perkembangan teknologi berdampak positif dalam rangka peningkatan kesejahteraan, kemajuan, dan peradaban manusia, namun perkembangan teknologi dan informasi ini juga berdampak negatif. Salah satunya adalah tindak kejahatan yang menggunakan media komputer dan internet yang dikenal dengan istilah kejahatan mayantara atau cybercrime. Penelitian ini menggunakan penelitian hukum normatif dan pendekatan perundang-undangan, konseptual, dan perbandingan. Bahwa hasil penelitian menunjukkan Jika dibandingkan dengan negara lain maka Indonesia mengalami keterlambatan dalam mengatur formulasi hukum mengenai cybercrime terkhusus cyber-terrorism. Selain itu penegakan hukum juga mengalami ketidakjelasan karena belum ada instrumen yang mengatur secara jelas dan tegas. Dalam konteks ini Indonesia harus menggunakan politik hukum pidana guna menyusun dan mengatur mengenai kejahatan cyber-terrorism dalam rangka penanggulangan kejahatan dunia maya. Oleh karena itu pemerintah harus segera membuat aturan atau rancangan undang-undang untuk mengantisipasi kejahatan cyber-terrorism.
Kata Kunci: Cybercrime; Cyber-terrorism; Politik Hukum Pidana.

Pendahuluan

Pesatnya perkembangan teknologi informasi membawa manusia ke dalam era digital. Teknologi dan informasi ini mengalami revolusi dengan ditemukannya piranti elektronik yang mengefisiensikan manusia untuk melakukan komunikasi. Kemajuan teknologi yang sedemikian pesat, menyebabkan perubahan kegiatan manusia dalam berbagai bidang ekonomi, sosial, dan budaya yang sedemikian cepat. Pada hakikatnya perubahan dalam perkembangan teknologi berdampak positif dalam rangka peningkatan kesejahteraan, kemajuan, dan peradaban manusia, namun perkembangan teknologi dan informasi ini juga berdampak negatif. Salah satunya adalah tindak kejahatan yang menggunakan media komputer dan internet yang dikenal dengan istilah kejahatan mayantara atau *cybercrime*. *Cybercrime* adalah kejahatan yang berhubungan dengan komputer, yaitu setiap perilaku ilegal yang memanfaatkan komputer atau sistem jaringan.[1]

Istilah kejahatan komputer lebih dahulu dikenal telah memberikan gambaran mengenai ruang lingkup kejahatan berbasis teknologi informasi. Terlebih lagi hingga saat ini dalam berbagai literatur istilah kejahatan komputer *(computer crime)* diidentikan atau disepadankan dengan istilah kejahatan siber *(cybercrime)*. Menurut NCIS *(National Criminal Intelligence Service)* Inggris sebagaimana dikutip Ade Marman Suherman, menjelaskan ada 13 (tiga belas) macam *cybercrime* sebagai berikut:[2] *political hackers, crackers, recreational hackers, denial of service attack, insider, virues, piracy, fraud, gambling, pornography, cyber-stalking, hate sites, dan criminal communications.* Kemudian jenis kejahatan yang masuk dalam kategori yang sama antara lain: *cyber pornography, hacking, carding, dan cyber-terrorism.*

Perkembangan *cybercrime* semakin meningkat, sekaligus modus operandinya semakin beragam. Seperti halnya kejahatan yang masih konvensional seperti pencurian, pengancaman, perjudian, bahkan tindak pidana terorisme bisa dilakukan melalui dunia maya. *Cybercrime* memiliki sifat transnasional dasar argumenasinya

[1] Shelia Maulida Fitri*, Ransomware Wannacry dan Tindak Pidana Terorisme Siber* (Magnum Pustaka Utama 2020).[19].

[2] Abdulah Wahid dan Mohammad Labib, *Kejahatan Mayantara* (Refika Aditama 2005).[70].

adalah karena tidak terbatas pada ruang dan waktu sehingga bukan hanya berimplikasi negatif kepada individu, tetapi juga berimplikasi besar bagi negara dan organisasi serta kepentingan yang dilindungi oleh negara melalui produk hukum. Salah satu yang menjadi tantangan besar dan perlu adanya antisipasi sejak dini yakni terorisme. Tindak terorisme ini bahkan sudah dilakukan mengunakan sarana teknologi dan masuk dalam salah satu jenis *cybercrime* yakni *cyber-terrorism*.[3]

Lewis memberikan definisi *cyber-terrorism* sebagai pengguna perangkat jaringan komputer untuk mematikan infrastruktur dan menganggu suatu pemerintahan bahkan warga negara. Dalam pengesahan ASEAN Convention on Counter Terrorism bahwasanya semua negara harus bersiap dalam segala hal untuk melakukan penanggulangan dan pencegahan tindak kejahatan terorisme dan melakukan bekerja sama dalam rangka meningkatkan masyarakat untuk memberantas serta melawan terorisme termasuk *cyber-terrorism*. *Cyber-terrorism* termasuk salah satu kejahatan luar biasa (extraordinary crime). Kejahatan *cyber-terrorism* berkorelasi dengan ideologi dan pencucian otak tentang paham negara dengan melakukan komunikasi secara aktif menggunakan sarana teknologi dan menjadi kegiatan utama yang dilakukan oleh suatu kelompok atau individu dalam melancarkan aksinya.[4]

Cyber-terrorism bisa menyerang apapun yang terhubung dengan internet terutama objek vital yang dimiliki oleh pemerintah yang dapat mengakibatkan rusaknya sistem bahkan dapat menimbulkan korban yang lebih besar dari tindak pidana terorisme yang dilakukan secara konvensional.[5] *Cyber-terrorism* merupakan bentuk kejahatan yang terstruktur dan sistematis yang berupa serangan terhadap sistem komputer, program komputer, dan data sehingga dapat menyebabkan kerugian besar yang dilakukan oleh suatu kelompok organisasi ataupun individu. Internet

[3] Fredayani, 'Alasan Pembentukan Kerja Sama Keamanan ASEAN-Australia dalam Menghadapi Isu Terorisme' (2019) 6 Insignia Journal of International Relations.[94–105].

[4] Nur Qalbi, Fitrah Marinda, & Rina Yulianti, 'Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir' (2020) 4 Jurnal Legislatif. [109-110].

[5] Agis Adam, 'Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik' (2014) II Lex Administratum.[3].

selain digunakan untuk masyarakat sebagai sarana informasi dan konunukasi juga bisa digunakan atau dimanfaatkan untuk akses propaganda dalam menyebarkan paham radikal yang bertujuan untuk meresahkan masyarakat. Pada hakikatnya propaganda menjadi langkah awal yang sangat krusial untuk mengarahkan dan memanipulasi pikiran sehingga sesuai dengan apa yang diharapkan oleh pelaku.

Berbicara mengenai kejahatan *cyber-terrorism* sudah barang tentu wajib membahas mengenai aturan hukumnya dalam rangka melakukan perlindungan terhadap masyarakat. Di Indonesia, tindak kejahatan terkhusus *cyber-terrorism* belum diatur secara tegas di dalam Undang-Undang. Memang, Indonesia sudah mempunyai aturan hukum mengenai transaksi elektronik yaitu dengan adanya Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Kemudian Indonesia juga mempunyai aturan hukum mengenai tindak pidana terorisme yakni dengan adanya 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.

Membahas mengenai aturan hukum tentang *cyber-terrorism* merupakan suatu hal yang memiliki tantangan tersendiri. Dikarenakan peraturan perundang-undangan yang mengatur tentang kejahatan *cyber-terrorism* belum ada secara tegas tertulis secara experssive verbist di dalam Undang-Undang. Maka dari itu, dalam melakukan penanggulangan terhadap kejahatan *cyber-terrorism* diperlukan politik hukum pidana. Politik hukum pidana oleh Sudarto diartikan sebagai usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi saat itu.[6] Selain itu politik hukum pidana adalah upaya masyarakat untuk menetapkan hukum dalam rangka mencegah kejahatan dan diarahkan pada penanggulangan secara komprehensif dari berbagai macam bentuk kejahatan di ruang maya (cyberspace).[7]

---

[6] Sudarto, *Hukum dan Hukum Pidana Indonesia* (Alumni 1996).[27].

[7] Dewi Bunga, 'Politik Hukum Pidana Terhadap Penanggulangan *Cybercrime'* (2019) 16 Journal Legislasi Indonesia.[4].

Menjawab problematika tersebut, diperlukan inisiatif untuk mengonstruksi aturan hukum mengenai *cyber-terrorism* secara detail guna memberikan kepastian hukum serta membantu aparat dalam melakukan penegakan hukum dengan menggunakan politik hukum pidana. Usaha dan kebijakan untuk membuat peraturan pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Maka dari itu, penulis berusaha menjawab tantangan tersebut, dengan penulisan karya tulis berjudul, "Penanggulangan Terhadap Kejahatan *Cyber-terrorism* Melalui Politik Hukum Pidana". Judul tersebut dipandang sangat penting karena adanya kekosongan hukum di Indonesia mengenai kejahatan *cyber-terrorism* dan mengingat kejahatan tersebut sangat luar biasa maka harus ada aturan yang mengakomodir kejahatan tersebut dalam Undang-Undang. dengan rumusan permasalahan sebagai berikut; Pertama, bagaimanakah penegakan hukum pidana terhadap kejahatan *cyber-terrorism* di Indonesia. Kedua, bagaimana model politik hukum pidana dalam penanggulangan kejahatan *cyber-terrorism* di Indonesia.

Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian normatif. Pengumpulan data dilakukan dengan cara studi dokumentasi terhadap data sekunder yang terdiri bahan hukum primer yang bersumber dari peraturan perundang-undangan, bahan hukum sekunder yang bersumber dari buku hukum dan karya ilmiah, serta bahan hukum tersier berupa kamus hukum. Penelitian ini menggunakan tiga pendekatan untuk memecahkan dan menjawab rumusan masalah yaitu pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan. Metode analisis data dalam penelitian ini menggunakan metode kualitatif, sedangkan hasil dari analisis disajikan secara deskriptif-preskriptif. Metode penarikan kesimpulan dalam penelitian ini menggunakan metode induktif.

Penegakan Hukum Pidana Terhadap Kejahatan *Cyber-terrorism* di Indonesia Studi Komparatif: Aturan Hukum Mengenai Penegakan Hukum Pidana Terkait *Cyber-terrorism* di Beberapa Negara

Pengaturan *cybercrime* di India dilakukan tersendiri dalam *The Information Technology Act 2000.* Dalam Bab IX tentang sanksi Pidana dan Peradilan, Pasal 43 diatur bahwa:

> *"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network".*

Terjemahan bebas:

> "Setiap orang dapat dipidana atas suatu perusakan pada komputer atau sistem komputer dan lain-lain tanpa ijin dari pemiliknya; atau setiap orang yang melakukan penyerangan terhadap komputer, sistem komputer atau jaringan komputer".

Kemudian secara tegas dalam pengaturan mengenai *cyber-terrorism* ada dalam ketentutan lebih tepatnya pada Pasal 43 huruf (e):[8]

> *"disrupts or causes disruption of any computer, computer system or computer network"*

Terjemahan bebas:

> "mengganggu atau menyebabkan gangguan pada komputer, sistem komputer dan jaringan komputer".

Bahwa dalam konteks kejahatan *cyber-terrorism* di India, secara tegas dan jelas seseorang akan menghadapi hukuman penjara seumur hidup jika pelaku mencoba menembus/ mengakses jaringan komputer tanpa izin, dengan tujuan untuk mengancam persatuan, keamanan atau kedaulatan bangsa.

Seperti dengan India, Singapura juga memiliki regulasi mengenai *cybercrime* yakni *The Computer Misue Act (CMA) 1993.* Singapura membedakan 4 bentuk tindak pidana yang berhubungan dengan komputer, yang sebagaimana diatur secara khusus dalam bab *(offences).* Ketentuan tersebut adalah sebagai berikut:

1. Unauthorised access to computer material

[8] Siddhi, 'The Information Technology Act 2000' (GeeksForGeeks, 2015) <http://cyberlawindia.com/wp-content/uploads/2015/03/The-Information-Technology-Act-2000.pdf>, dikunjungi pada tanggal 18 Maret 2023

2. *Unauthorised access with intent to commit or facilitate commission of further offences*
3. *Unauthorised modification of computer material*
4. *Unauthorised use or interception of computer service.*

Di singapura, setiap orang yang membantu melakukan kejahatan seperti yang sudah diuraikan diatas dianggap sebagai pelaku tindak pidana. Selain itu Singapura sudah mengakomodir kejahatan *cyber-terrorism* secara jelas. Subjek yang dapat dipidana tidak hanya pelaku di wilayahnya tetapi juga di luar wilayah Singapura. Bahkan polisi Singapura diizinkan menahan tanpa surat perintah penahanan terhadap pelaku. Kemudian dalam hal ini jika dibandingkan dengan Indonesia, Indonesia adalah negara yang paling terlambat dalam dalam mengatur tindak pidana dibidang teknologi dan informasi.

Analisis Penegakan Hukum Pidana Terhadap Kejahatan *Cyber terrorism* Melalui Sarana Penal.

Penggunaan hukum pidana (penal) di Indonesia sebagai sarana untuk menanggulangi kejahatan, nampaknya tidak menjadi persoalan. Hal ini terlihat dalam praktik perundang-undangan selama ini menunjukkan bahwa penggunaan hukum pidana merupakan bagian dari kebijakan yang diatut oleh Indonesia. Terlebih dalam konteks kejahatan *cyber-terrorism,* sarana penal sangat dibutuhkan karena ada asas *primum remedium,* megingat kejahatan ini tergolong kejahatan luar biasa. Tentunya ditunjang dengan landasan hukum yang jelas sehingga aparat tidak salah dalam mengambil tindakan hukum dalam proses penyelidikan, penyelidikan, dan penuntutan.

Sebelum membahas lebih mengenai *cyber-terrorism* maka penting untuk mendefinisikan apa itu *cyber-terrorism. Cyber-terrorism* adalah tindak pidana yang dilakukan melalui sarana komputer yang berimplikasi terjadinya kekerasan, kematian dan/atau kehancuran, dan menciptakan teror untuk tujuan memaksa pemerintah untuk mengubah arah kebijakannya. Bahwasannya kejahatan tersebut merupakan *dark side* kemajuan teknologi informasi. Pelaku teror atau komplotan teroris dengan kemajuan teknologi informasi kian berkembang lebih progresif. Pelaku teror menggunakan sarana internet untuk menjalankan tujuannya dengan

lebih efektif. Dampaknya sangat memungkinkan pengembangan organisasi yang bersifat lokal menjadi kelompok teror transnasional. Dengan menggunakan sarana internet, maka sudah barang tentu mereka dengan mudah melakukan koordinasi. Oleh karena itu terjadi pergeseran dari tahap evolusi terorisme yang serangannya bersifat nyata menuju pada serangan mayantara.[9]

Secara teroretik, tindak pidana siber memiliki karakteristik yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi, maupun tempat terjadinya suatu perkara sehingga membutuhkan penanganan khusus diluar KUHP. Indonesia sendiri pernah mengalami kasus *cyber-terrorism* yakni adanya serangan *Ransomware Wannacry*. Seperti yang dilansir dari berita *online* Liputan 6, bahwa serangan *Ransomware Wannacry* ini diketahui setelah sejumlah rumah sakit di Indonesia mengalami kendala teknis dalam sistem antreannya. Rumah sakit tersebut adalah RS Harapan Kita dan Rumah sakit Dharmais.[10] Lebih tepatnya pada Mei 2017, bahwa dua rumah sakit tersebut mengeluhkan gangguan sistem komputer yang berkaitan dengan administrasi rumah sakit sehingga menyulitkan pelayanan medis bagi pasien. Bahwa setelah ditelisik ternyata disebabkan oleh serangan *Ransomware Wannacry. Ransomware Wannacry* merupakan *malware* yang menyerang komputer korban dengan cara mengunci komputer korban atau mengenskrip semua file yang ada sehingga tidak bisa diakses kembali. Enskrip ini bisa ditebus dengan cara mengirimkan sejumlah uang kepada pemilik, virus dalam bentuk virtual seperti *bitcoin.*[11] Serangan siber ini bersifat tersebar dan masif serta menyerang *critical resource* (sumber daya sangat penting). Sehingga serangan ini memanfaatkan bisa dikategorikan sebagai *cyber-terrorism*.

---

[9] Ufran, 'Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism' (2014) 43 Jurnal MMH.[503].

[10] Iskandar, 'Penjelasan Pakar Soal Serangan Wannacry di Indonesia' (Liputan6, 2017) <https://www.liputan6.com/tekno/read/2950477/penjelasan-pakar-soal-serangan-wannacry-di-indonesia>, dikunjungi pada pada tanggal 17 Maret 2023

[11] Muhammad Syadri, 'Ayo Kenali Teroris Baru dari Virus Ransomeware bernama Wanna Cry' (JawaPos, 2017)<https://www.jawapos.com/teknologi/14/05/2017/ayo-kenali-teroris-baru-dari-virus-ransomware-bernama-wannacry>, dikunjungi pada tanggal 17 Maret 2023

Berbicara mengenai penegakan hukum terhadap kejahatan *cyber-terrorism* di Indonesia terhadap kasus serangan *ransomware wannacry* tidak mengalami kejelasan. Pada awal kemunculannya, sebenarnya pemerintah Indonesia menyatakan menggandeng FBI dalam rangka mengusut tuntas kasus ini mengingat pelaku melakukan penyerangan secara global dan sporadik ke seluruh dunia termasuk Indonesia.[12] Untuk kasus yang terjadi di Indonesia, virus ini menyerang sejumlah jaringan komputer dan meminta tebusan Rp. 4.000.000,- untuk mengembalikan komputer ke sediakalanya. UU ITE melalui Pasal 30 dan Pasal 32 sesungguhnya memiliki dimensi pengaturan yang bisa mengakomodir penegakan hukum terhadap serangan *cyber-terrorism* melalui virus *ransomware wannacry* dengan sanksi sebagaimana diatur dalam Pasal 46 dan Pasal 48 dengan ancaman hukuman penjara maksimal 10 tahun dan denda maksimal Rp. 5.000.000.000,-. Namun rumusan delik dalam kedua pasal *a quo* masih sangat sederhana sehingga lebih tepat ditegakan terhadap pelaku *cyber-terrorism* yang menyerang perseorangan, bukan terhadap serangan yang masif, meluas, dan terlebih menyerang objek vital negara. Kemudian jika menggunakan instrumen UU Terorisme bahkan belum ada pengaturannya, jika dilihat dari sikap batin atau motif, serangan *ransomware wannacry* yang masif dan meluas bukan masuk dalam tindak pidana terorisme sebagaimana dalam Pasal 1 angka 2 UU Terorisme karena tidak memenuhi kualifikasi motif ideologi dan politik meskipun sesungguhnya sama-sama mengakibatkan gangguan keamanan.

Sebagaimana yang sudah diuraikan, maka hingga saat ini belum ada kejelasan bagaimana upaya melalui sarana penal sebagai tindakan nyata dari aparatur penegakan hukum Indonesia guna menindak tegas kejahatan *cyber-terrorism* di Indonesia, mengingat pelaku susah untuk ditemukan karena kejahatan ini berdimensi transnasional sehingga susah untuk dilakukan pelacakan. Selain itu, peraturan yang kurang jelas juga menghambat proses penyelidikan dan penyidikan bahkan penuntutan. Serangan ini juga menimbulkan ketakutan terhadap masyarakat

[12] Juven Martua, 'Polri Akan Gandeng FBI buru pelaku serangan virus Wannacry (Merdeka. Com, 2017)<https://www.merdeka.com/peristiwa/polri-akan-gandeng-fbi-buru-pelaku-serangan-virus-wannacrypt.html>, dikunjungi pada tanggal 17 Maret 2023.

luas tidak hanya untuk instansi pemerintahan namun pada sektor bisnis swasta. Disamping itu, dalam penegakannya instrumen peraturannya juga belum ada secara tegas *experssive verbist* undang-undang mana yang digunakan aparat guna melaksanakan penegakan hukum.

Model Politik Hukum Pidana Dalam Penanggulangan Kejahatan *Cyber-terrorism* di Indonesia

Politik Hukum menurut Mahfud MD adalah *legal policy* atau garis kebijakan resmi tentang hukum yang akan diberlakukan baik dengan pembuatan hukum baru maupun dengan penggantian hukum lama, dalam rangka mencapai tujuan negara. Dengan demikian, politik hukum merupakan pilihan tentang hukum yang akan diberlakukan sekaligus pilihan tentang hukum yang akan dicabut atau tidak diberlakukan yang kesemuanya dimaksudkan untuk mencapai tujuan negara seperti yang tercantum dalam pembukaan UUD 1945.[13] Kemudian Satjipto Raharjo mendefinisikan politik hukum sebagai aktivitas memilih dan cara yang hendak dipakai untuk mencapai suatu tujuan sosial dengan hukum tertentu di dalam masyarakat.[14] Sudarto juga mengemkakan pendapatnya mengenai politik hukum bahwa politik hukum merupakan upaya untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu waktu.[15]

Istilah lain politik hukum pidana adalah kebijakan hukum pidana. Politik hukum pidana itu pada intinya bagaimana hukum pidana dapat dirumuskan dengan baik dan memberikan pedoman kepada pembuat undang-undang dan pelaksanaan hukum pidana. Kebijakan legislatif merupakan tahap yang sangat krusial dan menentukan bagi tahapan-tahapan selanjutnya, karena pada saat perundang-undangan pidana hendak dibuat, maka sudah ditentukan tujuan yang hendak dicapai. Dalam konteks ini ruang lingkup kebijakan legislasi menekankan pada upaya berikut:

---

[13] Moh. Mahfud MD, *Politik Hukum di Indonesia* (PT. RajaGrafindo Persada 2009).[1].
[14] Satjipto Raharjo*, Ilmu Hukum* (PT Citra Aditya Bakti 1991).[352-353].
[15] Sudarto*, Hukum dan Hukum Pidana* (Alumni 1986).[151].

1. Penggantian perundang-undangan warisan kolonial dan hukum nasional yang sudah tidak sesuai dengan perkembangan masyarakat;
2. Menyempurnakan peraturan perundang-undangan yang sudah ada namun tidak sesuai dengan tuntutan dan kebutuhan masyarakat;
3. Membentuk peraturan perundang-undangan baru yang sesuai dengan tuntutan dan memenuhi kebutuhan hukum masyarakat.[16]

Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal *(criminal policy)*. Sebagian dari politik kriminal, politik hukum pidana identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana.[17] Dalam konteks penanggulangan *cybercrime* terkhusus *cyber-terrorism* yang menjadi fokus pembahasan maka Indonesia perlu melakukan kriminalisasi perbuatan tersebut baik dalam UU ITE dan UU Pemberantasan Terorisme. Secara konseptual kriminalisasi merupakan proses menjadikan perbuatan yang tadinya bukan merupakan bukan kejahatan menjadi kejahatan melalui peraturan dalam peraturan perundang-undangan. Pertimbangan dilakukannya kriminalisasi perbuatan kejahatan adalah berdasarkan pertimbangan fakta maraknya kasus *cybercrime* di Indonesia.

Antisipasi sejak dini harus diupayakan yakni dengan produk hukum yang notabene kejahatan yang canggih saat ini masuk ke dalam celah hukum yang sulit ditanggulangi, oleh karenanya, politik hukum pidana menjadi sarana dan alternatif guna melakukan pencegahan dan penanggulangan terhadap kejahatan dunia maya. Dalam mengonstruksi pun perlu adanya telaah yang komperhensif dimana menentukan obyek dan subjeknya. Indonesia sendiri memang sudah mempunyai produk hukum untuk mengantisipasi *cybercrime* terkhusus *cyber-terrorism* tetapi dalam undang-undang *a quo* belum diatur secara tegas pengaturan spesifik mengenai kejahatan *cyber-terrorism*.

---

[16] Ruslan Renggong, *Hukum Pidana Khusus: Memahami delik-delik di Luar KUHP* (Prenadamedia Grup).[7-8].

[17] Hanafi Amrani, *Politik Pembaharuan Hukum Pidana* (UII Pers 2019).[4-5].

Mengingat Politik hukum pidana merupakan bagian dari politik kriminal. Politik kriminal merupakan pengaturan atau penyusunan secara rasional usaha-usaha pengendalian kejahatan oleh masyarakat. Politik kriminal bisa diartikan dalam beberapa lingkup. *Pertama,* dalam arti sempit digambarkan sebagai keseluruhan asas dan metode yang menjadi dasar dari reaksi terhadap pelanggaran hukum yang berupa pidana. *Kedua,* dalam artian luas kebijakan kriminal merupakan keseluruhan fungsi dari aparatur penegak hukum, termasuk cara kerja polisi, jaksa, dan hakim. *Ketiga,* dalam konteks yang lebih luas kebijakan kriminal adalah keseluruhan kebijakan melalui peraturan perundang-undangan dan badan-badan resmi, yang bertujuan untuk menegakkan norma sentral dari masyarakat.[18]

Berbicara masalah pemberantasan *cyber-terrorism,* bahwa dalam melakukan penanggulangan kejahatan ini, perlu adanya inventarisasi masalah-masalah yang menjadi kendala, guna mengonstruksi sebuah peraturan mengenai pencegahan dan penanggulangan *cyber-terrorism*, yakni sebagai berikut:

a. Belum adanya benang merah definisi terorisme dan terorisme siber mengingat istilah terorisme siber belum banyak dipakai dalam literatur di Indonesia;
b. Masih belum jelas formulasi hukum yang dapat mengakomodir tindak kejahatan *cyber-terrorism*. Walaupun Indonesia sudah mempunyai instrumen hukum yakni UU ITE dan UU Terorisme, tetapi jangkauannya masih sangat lemah;
c. Perlu adanya kajian komperhensif mengenai kejahatan *cyber-terrorism,* mengingat kejahatan ini memiliki karakteristik yang berbeda dengan tindak pidana lainnya, sebagai contoh bahwa kejahatan ini bisa melintasi batas yurisdiksi negara, sementara eksistensi perjanjian internasional mengenai *law enforcement* terhadap kejahatan *cyber-terrorism* masih sangat terbatas;
d. Sumber daya aparat penegak hukum yang masih minim pengetahuannya terhadap perkembangan kejahatan di dunia maya;
e. Pemerintah masih kurang memberikan perhatian terhadap permasalahan ini, sebagai buktinya adalah masih lemahnya UU mengenai *cybercrime* terkhusus *cyber-terrorism.*

Oleh karena itu, dengan kebijakan kriminal muncul dua masalah sentral dengan menggunakan sarana penal yaitu masalah: *Pertama,* penentuan perbuatan apa yang seharusnya dijadikan tindak pidana (kriminalisasi), dan *kedua,* penentuan

[18] Sudarto, *Kapita Selekta Hukum Pidana* (Penerbit PT Alumni 1981).[113-114].

sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.[19] Kemudian pencegahan dan penanggulangan kejahatan dengan sarana hukum pidana, fungsionalisasi dan operasionalisasi dapat dilakukan melalui tahapan-tahapan. Antara lain:[20]

1. Tahap Fromulasi (Kebijakan Legislatif)

Tahap formulasi merupakan tahap penegakan hukum *in abstracto* oleh badan pemuat undang-undang. Tahap ini bisa juga disebut tahap kebijakan legislatif. Dalam kebijakan legislatif ini adalah proses perencanaan atau program dari pembuat undang-undang mengenai apa yang akan dilakukan dalam menghadapi problem tertentu dengan cara bagaimana melakukan atau melaksanakan sesuatu yang telah direncanakan atau diprogramkan. Pokok-pokok dalam kebijakan formulasi hukum pidana terdiri atas; a). Perumusan tindak pidana; b). perumusan pertanggungjawaban pidana; dan c). perumusan sanksi.

2. Tahap Aplikasi (Kebijakan Yudisial)

Tahap aplikasi merupakan penerapan hukum pidana oleh aparat penegak hukum mulai dari kepolisian sampai pengadilan. tahap kedua ini disebut juga kebijakan yudikatif. Bagian ini tidak dapat dipisahkan dari sistem peradilan pidana atau *criminal justice system* yang terintegrasi.

3. Tahap Eksekusi (kebijakan eksekutif)

Tahap eksekusi merupakan tahap pelaksanaan hukum pidana secara konkret oleh aparat pelaksana pidana. Tahap ini disebut kebijakan administratif. Dengan adanya tahap formulasi, maka upaya pencegahan kejahatan bukan hanya tugas aparat penegak hukum, tetapi juga tugas dari aparat pembuat hukum, bahkan kebijakan legislatif adalah tahap yang paling strategis dari upaya penanggulangan dan pencegahan.

Berkaitan dengan model politik hukum pidana dalam *criminal policy,* bahwa orientasi hukum pidana adalah agar masyarakat terlindungi oleh hukum. Tujuan hukum ini tidak terlepas dari dua fungsi hukum pidana, yaitu: fungsi primer, sebagai

[19] Barda Nawawi Arief, *Kebijakan Legislatif, dalam Penanggulangan Kejahatan dengan Pidana Penjara* (Badan Penerbit UNDIP 1996).[35].

[20] Dey Ravena, *Kebijakan Kriminal* (Balebad Dedikasi Prima 2017).[I56].

sarana untuk mencegah kejahatan dan fungsi sekunder, yakni menindak pelaku kejahatan. Yang perlu di garis bawahi adalah fungsi sekunder akan diterapkan jika fungsi primer tidak mampu dilaksanakan. Dan aturan hukum harus jelas dan tegas mengatur secara detail rumusan delik, pertanggungjawaban, dan sanksi. Selain itu, model politik hukum pidana dalam penanggulangan kejahatan *cyber-terrorism,* bahwa kebijakan hukum pidana dalam rangka membentuk perundang-undangan, diarahkan pada pada pembentukan substansi hukum yang bersifat responsif dan mampu menjadi sarana pembaharuan serta pembangunan bagi kepentingan nasional. Lalu, kebijakan hukum pidana disamping mengkaji masalah perundang-undangan pidana yang berlaku, juga menentukan seberapa jauh perundang-undangan itu diubah. Terakhir adalah kebijakan hukum pidana pada hakikatnya merupakan bagian dari kebijakan penegakan hukum.

Kesimpulan

Indonesia menjadi sorotan internasional karena masih lambannya dalam mengatur tindak pidana dibidang teknologi dan informasi. Jika dibandingkan dengan beberapa negara yakni Singapura dan India, pengaturan hukum *cybercrime* terkhusus *cyber-terrorism* jauh tertinggal. India mempunyai aturan hukum mengenai *cybercrime* sekaligus mengakomodasi kejahatan *cyber-terrorism* dengan adanya *The Information Technology Act 2000.* Sedangkan Singapura juga sudah memiliki payung hukum yakni dengan adanya *The Computer Misue Act (CMA) 1993* yang secara tegas juga sudah mengakomodir kejahatan *cyber-terrorism* bahkan cakupanya sudah sangat luas mengenai subjek dan yurisdiksi. Walaupun demikian, Indonesia sebenarnya juga sudah mempunyai produk hukum yakni dengan adanya Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Tetapi cakupan mengenai subjek dan yurisdiksi masih sangat terbatas. Kemudian dalam hal penegakan hukum melalui sarana penal, aparat penegak hukum dalam menjalankan tugasnya mengalami ketidakjelasan, karena pengaturannya masih belum diatur scara jelas dan tegas di dalam undang-undang yang mana dalam konteks *cyber-terrorism.*

Disamping itu pelaku susah untuk ditemukan karena kejahatan ini berdimensi transnasional sehingga susah untuk dilakukan pelacakan. Selain itu, peraturan yang kurang jelas juga menghambat proses penyelidikan dan penyidikan bahkan penuntutan. Serangan ini juga menimbulkan ketakutan terhadap masyarakat luas tidak hanya untuk instansi pemerintahan namun pada sektor bisnis swasta.

Model politik hukum pidana untuk penanggulangan kejahatan *cyber-terrorism* harus dikaji secara komperhensif. Sebelum melakukan konstruksi hukum tentunya harus menginventarisasi permasalahan. Pada intinya inventarisasi masalah yang ditemukan adalah belum adanya benang merah definisi terorisme dan terorisme siber, belum jelasnya formulasi hukum, memahami karakteristik dari kejahatan *cyberterrorism*, sumber daya aparat penegak hukum yang masih minim pengetahuannya terhadap perkembangan kejahatan *cyber-terrorism.* Kemudian berbicara mengenai kebijakan hukum pidana maka harus melewati beberapa tahapan yakni tahap formulasi, tahap aplikasi, dan tahap eksekusi. model politik hukum pidana dalam penanggulangan kejahatan *cyber-terrorism,* bahwa kebijakan hukum pidana dalam rangka membentuk perundang-undangan, diarahkan pada pada pembentukan substansi hukum yang bersifat responsif dan mampu menjadi sarana pembaharuan serta pembangunan bagi kepentingan nasional. Lalu, kebijakan hukum pidana disamping mengkaji masalah perundang-undangan pidana yang berlaku, juga menentukan seberapa jauh perundang-undangan itu diubah. Terakhir adalah kebijakan hukum pidana pada hakikatnya merupakan bagian dari kebijakan penegakan hukum.

Daftar Bacaan

Buku

Abdulah Wahid dan Mohammad Labib, *Kejahatan Mayantara* (Refika Aditama 2005).

Barda Nawawi Arief, *Kebijakan Legislatif, dalam Penanggulangan Kejahatan dengan Pidana Penjara* (Badan Penerbit UNDIP 1996).

Dey Ravena, *Kebijakan Kriminal* (Balebad Dedikasi Prima 2017).

Hanafi Amrani, *Politik Pembaharuan Hukum Pidana* (UII Pers, 2019).

Moh. Mahfud MD, *Politik Hukum di Indonesia* (PT. RajaGrafindo Persada 2009).

Ruslan Renggong, *Hukum Pidana Khusus: Memahami delik-delik di Luar KUHP* (Prenadamedia Grup).

Satjipto Raharjo*, Ilmu Hukum* (PT Citra Aditya Bakti 1991).

Shelia Maulida Fitri*, Ransomware Wannacry dan Tindak Pidana Terorisme Siber* (Magnum Pustaka Utama 2020).

Sudarto, *Kapita Selekta Hukum Pidana* (Penerbit PT Alumni 1981).

_____ *, Hukum dan Hukum Pidana* (Alumni 1986).

_____ , *Hukum dan Hukum Pidana Indonesia* (Alumni 1996).

Jurnal

Agis Adam, 'Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik', (2014) II Lex Administratum.

Dewi Bunga, 'Politik Hukum Pidana Terhadap Penanggulangan *Cybercrime'*, (2019) 16 Journal Legislasi Indonesia.

Fredayani, 'Alasan Pembentukan Kerja Sama Keamanan ASEAN-Australia dalam Menghadapi Isu Terorisme'. (2019) 6 Insignia Journal of International Relations.

Nur Qalbi, Fitrah Marinda, & Rina Yulianti, 'Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir', (2020) 4 Jurnal Legislatif.

Ufran, 'Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism', (2014) 43 Jurnal MMH 4.

Laman

Iskandar, 'Penjelasan Pakar Soal Serangan Wannacry di Indonesia'(Liputan6,2017) <https://www.liputan6.com/tekno/read/2950477/penjelasan-pakarsoal-serangan-wannacry-di-indonesia>, dikunjungi pada pada tanggal 17 Maret 2023.

Juven Martua, 'Polri Akan Gandeng FBI buru pelaku serangan virus Wannacry (Merdeka.Com,2017)<https://www.merdeka.com/peristiwa/polri akan-gandeng-fbi-buru-pelaku-serangan-virus-wannacrypt.html>,dikunjungi pada tanggal 17 Maret 2023.

Muhammad Syadri, 'Ayo Kenali Teroris Baru dari Virus Ransomeware bernama WannaCry'(JawaPos,2017)<https://www.jawapos.com/teknologi/14/05/2017/ayo-kenali-teroris-baru-dari-virus-ransomware-bernama-wannacry>, dikunjungi pada tanggal 17 Maret 2023.

Siddhi, 'The Information Technology Act 2000' (GeeksForGeeks,2015) <http://cyberlawindia.com/wp-content/uploads/2015/03/The-Information-Technology-Act-2000.pdf>, dikunjungi pada tanggal 18 Maret 2023

Perundang-undangan

Undang-Undang Nomor 19 Tahun 2016 Tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Nomor 4843 Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

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, Tambahan Lembaran Negara Republik Indonesia Nomor 4284, Tambahan Lembaran Negara Republik Indonesia Nomor 6216.

--halaman ini sengaja dibiarkan kosong--