

sapta4

by Saptaning Paminto

Submission date: 03-Jan-2022 07:02PM (UTC+1000)

Submission ID: 1737058792

File name: BAB_I_JAPUNG.pdf (253.53K)

Word count: 3651

Character count: 24764



**ANALISIS PENEGAKAN HUKUM DENGAN MENGGUNAKAN
TEKNOLOGI INFORMASI SEBAGAI AKSI DAN SARANA TERHADAP
PELAKU CYBER TERORISM SEHINGGA MENIMBULKAN BENTUK**

SAPTANING RUJU PAMINTO
DOSEN FAKULTAS HUKUM
UNIVERSITAS SURYAKANCANA



POST GRADUATE PROGRAM
UIN SUNAN GUNUNG DJATI
BANDUNG INDONESIA
2018

BAB I

PENDAHULUAN

A. Latar Belakang Penelitian.

Negara Republik Indonesia berdasarkan Pasal 1 Ayat (3) Undang-Undang Dasar 1945 adalah negara hukum (*Rechtstaat*), Sehingga hukum dijadikan sebagai bahan pijakan dalam menjalankan fungsinya terhadap Pengadilan dan penyelesaian berbagai persoalan roda kehidupan bermasyarakat, berbangsa dan bernegara.

Dengan meningkatnya proses modernisasi akibat ditemukannya alat-alat komunikasi, transportasi dan informatika modern hal ini menuntut nilai-nilai dan norma baru dalam kehidupan nasional dan antar-bangsa. Bidang ekonomi pendorong utama globalisasi adalah meningkatnya arus informasi, uang dan perusahaan multinasional yang bergerak cepat melalui pasar bebas, arus modal dan penanaman modal dari luar negeri, yang dapat dikatakan bahwa globalisasi tidak bersifat fakultatif (*change is not optional*).¹

Kemajuan ilmu pengetahuan dan teknologi yang sangat pesat dibidang telekomunikasi, informasi dan komputer telah menghasilkan suatu aplikasi kehidupan serba modern. **Teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global, perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas (*borderless*)** menurut ahli **Kenichi Ohmae** dalam bukunya “*The borderless world*” yang mengungkapkan dunia

¹ Muladi, *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, The Habibie center, Jakarta, 2002, hlm. 155-156.

tanpa batas dimana kekuatan dan strategi di dalam ekonomi yang saling mengikat, sejalan dengan ungkapan itu, ia mengemukakan terdapat lima faktor yang menentukan yang berdampak dalam ekonomi global yang disebutnya dengan (5C) yaitu:

- a. *Customer* (pelanggan) sebagai kekuatan mereka yang mulai muncul dimana mereka tidak khawatir untuk mendapatkan produk yang dibutuhkan, yang mereka pedulikan adalah hal yang berkaitan kualitas, harga, desain, nilai dan daya tariknya bagi anda sebagai konsumen. Oleh karena yang menjadi tantangan adalah kemampuan perusahaan untuk menciptakan nilai bagi pelanggan.
- b. *Competition* (persaingan) sebagai kekuatan penyebaran teknologi dimana teknologi baru menjadi tersedia secara umum dengan lebih cepat, waktu semakin menjadi elemen yang kritis di dalam strategi, walaupun disadari bahwa tidak ada perusahaan yang dapat menyembunyikan semua teknologi kritis dari jangkauan pesaing di seluruh dunia.
- c. *Company* (perusahaan) sebagai kekuatan untuk bersaing di pasar global akan berdampak untuk menanggung biaya tetap yang membesar seperti halnya pemanfaatan teknologi informasi menjadi biaya tetap dan akan menjadi variabel melalui penyesuaian di dalam tingkat investasi, sedangkan dalam jangka panjang harus ada kemampuan untuk meningkatkan penjualan.
- d. *Currency* (mata uang) sebagai kekuatan yang harus dipertimbangkan karena nilai mata uang begitu mudah berubah. Oleh karena itu perusahaan internasional berusaha menetralkan dampak mata uang tersebut.

e. *Country* (negara) sebagai kekuatan dimana perusahaan berada akan selalu berusaha mendekatkan kepada langganannya sekaligus juga berusaha untuk menetralkan dampak mata uang dan juga kemungkinan proteksionisme. Bagi perusahaan yang benar-benar global yang dapat mencapai “lokalisasi global” yaitu menjadi orang dalam (insider) sebanyak mungkin seperti perusahaan lokal tetapi tetap mencapai manfaat dari operasi skala dunia.²

Dengan menyebabkan perubahan sosial, budaya, ekonomi dan pola penegakan hukum secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia. Sekaligus menjadi sarana efektif perubahan melawan hukum.³

Melalui globalisasi informasi yang benar-benar sudah memasuki rumah, sekolah dan institusi agama, masyarakat diseret untuk dapat mengakses dan menikmat berbagai bentuk informasi revolusi kultural di negara-negara atau bangsa-bangsa lain dimuka bumi. Masyarakat terus menerus disajikan hidangan bernama “menu perubahan” yang mengarah kepada masyarakat agar menjadi manusia lain, corak manusia yang sesuai dengan target dari “rezim” globalisasi.⁴

Berbagai modus operandi baru dalam bidang telekomunikasi, informasi dan komputer mulai bermunculan, hal ini seolah membenarkan adagium bahwa “dimana ada

² Dikutip dari Internet <http://hj-amanah.blogspot.co.id/2015/09/ekonomi-global-dalam-dunia-tanpa-batas.html> pada hari Senin, Tanggal 03-03-2017 14:11 WIB

³ Departemen Komunikasi dan Informatika Republik Indonesia, *Menuju Kepastian Hukum di Bidang : Informasi dan Transaksi Elektronik*, Jakarta, 2007, hlm.1.

⁴ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005, hlm. 2.

masyarakat, di situ ada ada kejahatan” sehingga diperlukan bukti yang sifatnya digital untuk dapat mengungkapnya.

1 Pembangunan Nasional di Indonesia telah mencapai era tinggal landas. Hal ini antara lain diidentifikasi oleh semakin meningkatnya dua faktor utama yang dianggap sebagai kunci keberhasilan pembangunan dalam rangka memenuhi tuntutan era globalisasi, yaitu pertumbuhan ekonomi dan perkembangan pemanfaatan Ilmu Pengetahuan dan Teknologi (IPTEK). Salah satu produk IPTEK yang kecanggihannya berkembang pesat dan hampir menguasai seluruh aspek kehidupan masyarakat modern adalah teknologi komputer.⁵

1 Penggunaan teknologi internet banyak menyelesaikan persoalan yang rumit secara efektif dan efisien. Kecanggihan teknologi ini juga berpotensi membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku. Penggunaan teknologi internet telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali yaitu dunia maya, dunia yang tanpa batas atau realitas virtual (*virtual reality*). Inilah sebenarnya yang dimaksud dengan *Borderless World*.⁶

1 Diantara banyaknya manfaat dari perkembangan teknologi informasi dan komunikasi, muncul sisi negatif dengan mulai berjamurannya kejahatan yang dilakukan dengan menggunakan sarana teknologi informasi dan komunikasi. Dampak negatif dari perubahan pola perilaku pada era kehidupan global

⁵ Kata Pengantar Barda Nanawi Arief., dalam *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer* oleh Al. Wisnubroto, Universitas Atma Jaya.hlm 2.

⁶ Ahmad M.Ramli. *Cyber Law dan HAKI dalam Sistem Hukum di Indonesia*. Yogyakarta, 2004, hlm 1.

¹ tersebut nampak dari berkembangnya kriminalitas baik secara kuantitatif maupun kualitatif. Kini mulai muncul berbagai jenis kejahatan dengan dimensi baru seperti penyalahgunaan komputer, kejahatan perbankan dan lain sebagainya yang semakin sulit untuk ditanggulangi.⁷

Perkembangan teknologi dan informasi membuka peluang luas untuk membuat, memperoleh dan menyebarkan pesan secara interaktif dan luas. Peluang ini bisa dimanfaatkan untuk kepentingan yang positif maupun negatif. Pemanfaatan internet secara negatif, diantaranya untuk kepentingan teroris. Kegiatan terorisme meliputi penyebaran propaganda dan rasa takut, pengrekrutan, penyediaan logistik, pelatihan pembentukan para militer secara melawan hukum, perencanaan, serangan teroris, persembunyian dan perdanaan. Kini sebagai besar kegiatan tersebut dapat dilakukan dengan memanfaatan internet.⁸

¹ Salah satu masalah *cyber crime* yang sangat meresahkan dan mendapat perhatian baik dari kalangan nasional maupun kalangan internasional adalah masalah *Cyberterrorism*. Jenis *Cyberterrorism* di bidang *cyber crime* ini sering diartikan sebagai suatu aksi kejahatan terorisme yang menggunakan sarana teknologi dan informasi, elektronik, tujuannya melumpuhkan infrastruktur secara nasional, seperti energi, transportasi, untuk menekan/mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil.

Cyberterrorism juga sering disebut, kejahatan yang dilakukan dengan membuat gangguan, perusakan atau

⁷ Kata Pengantar Barda Nanawi Arief, dalam *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer* oleh Al. Wisnubroto, Universitas Atma Jaya Yogyakarta

⁸ Petrus Reinhard Golose, *Invasi Terorisme Ke Cyberspace*, Yayasan Pengembangan kajian Ilmu Kepolisian (YPKIK), Jakarta, 2015,hlm 1.

penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet (*cyber sabotage and exortion*) Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program komputer tertentu sehingga data, program komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana dikehendaki oleh pelaku.⁹

Cyberterrorism telah banyak terjadi baik di negara Indonesia maupun negara-negara lainnya. Dari data yang diperoleh mengenai kejahatan *Cyberterrorism* tersebut, Dalam hal ini, penulis tertarik untuk melakukan penelitian dan mengkaji aspek hukum *Cyberterrorism* dalam perspektif Undang-undang Informasi Transaksi Elektronik yang sering disingkat (ITE), Sehingga Penulis mengambil judul “**Penegakan Hukum Terhadap Pengguna Cyberspace Sebagai Sarana Kejahatan Cyberterrorism Dihubungkan Dengan Undang - Undang Nomor 19 Tahun 2016 Tentang Informasi Transaksi Elektronik**”

⁹ Ali Juliano Gema, sebagaimana di kutip oleh Abdul Wahid dan Mohammad Labib, dalam buku Sutaman, Kata Pengantar dari Khoiden, *Cyber Crime, Modus Operandi dan Penangulangannya*. LeksBang komputer PRESSindo Jogjakarta. 2007. hlm. 83.

B. Identifikasi Masalah.

Dalam membahas hal – hal yang berhubungan dengan Penegakan Hukum Terhadap Pelaku Kejaharan *Cyberterrorism* yang dikaji menurut Undang-Undang ITE (Informasi, Transaksi dan Elektronik) maka penulis mengadakan pembatasan permasalahan sebagai berikut :

1. Apa latar belakang terjadinya tindak pidana *Cyberterrorism* di Indonesia ?
2. Bagaimana Implementasi penegakan hukum terhadap Pelaku tindak pidana *Cyberterrorism* ?
3. Apa yang menjadi kendala dan hambatan dalam penegakan hukum pelaku *Cyberterrorism* ?

C. Maksud dan Tujuan Penelitian.

1. Untuk memahami cara kerja kejahatan *Cyberterrorism* sehingga mengetahui sistem kejahatan *Cyberterrorism* .
2. Untuk memperoleh pemahaman tentang kejahatan *Cyberterrorism* dalam perspektif perbuatan melawan hukum Khususnya di indonesia.
3. Untuk mengetahui Penegakan pidana hukum terhadap Pelaku *Cyberterrorism* dalam dunia maya.

D. Kegunaan Penelitian.**1. Kegunaan Teoritis.**

- a. Diharapkan dapat memberikan wawasan yang luas untuk penulis dalam mengembangkan wawasan keilmuan khususnya dalam bidang *Cyberterrorism* .
- b. Mengembangkan pemikiran yang kritis untuk para pembaca dan sebagai instrumen bertambahnya informasi tentang cara kerja kejahatan *Cyberterrorism* .
- c. Diharapkan dapat memberikan pembelajaran, khususnya dalam penanganan kejahatan *Cyberterrorism* .

2. Kegunaan Praktis.

- a. Mengoptimalkan perkembangan pemahaman penulis dalam menambah refensi ilmu pengetahuan yang khususnya dalam penegakan *Cyberterrorism* .
- b. Diharapkan menjadi bahan pertimbangan dalam rangka mengintegrasikan kontroversi mengenai *Cyberterrorism* .
- c. Diharapkan pembaca dapat mengetahui pentingnya memahami tinjauan yuridis serta prosedur tentang pelaksanaan kejadian *Cyberterrorism* .

E. Kerangka Pemikiran.

1. Negara Hukum.

Indonesia sebagai negara hukum yang demokratis merupakan pernyataan politik hukum bangsa Indonesia yang tercermin dalam Undang-Undang Dasar 1945 Pasal 1 Ayat (1) yang menyatakan “ Negara Indonesia ialah Negara Kesatuan yang berbentuk Republik” Ayat (2) “Kedaulatan berada di tangan rakyat dan dilaksanakan menurut Undang-Undang Dasar” dan Ayat (3) berbunyi “Negara Indonesia adalah Negara Hukum”.¹⁰

Masyarakat tidak dapat dipisahkan dari hukum. Seperti yang diungkapkan oleh **Cicero** sebagai *ubi societas ibi ius* yang berarti “ diaman ada masyarakat, di situ ada hukum”. Hukum diperlukan oleh masyarakat itu sendiri.

Salah satu tugas hukum adalah melindungi kepentingan masyarakat, karena itu hukum positif dalam suatu tempat dipengaruhi oleh susunan dan keadaan masyarakat. Dalam realita, hukum tidak selalu menjadi lawan dari ketertiban, melainkan dapat menjadi lawan dari ketertiban itu sendiri. Karenanya penegakan hukum dalam suatu negara selalu

¹⁰ Dedi Mulyadi, *Kebijakan Legislasi, Tentang Sanksi Pidana Pemilu Legislatif di Indonesia dalam Perspektif demokrasi*, Gramata Publishing, Jakarta, 2012, hlm. 1.

berhubungan dengan kekuasaan hukum dan kekuasaan politik.¹¹

2. Hukum Pidana Indonesia.

Hukum pidana merupakan bagian dari sistem hukum atau sistem norma-norma. Sebagai sebuah sistem, hukum pidana mempunyai sifat umum dari suatu sistem yaitu menyuruh (*wholes*), memiliki beberapa elemen, semua elemen saling terikat dan kemudian membentuk struktur.¹²

Kebijakan hukum pidana adalah merupakan bagian dari pembaharuan hukum pidana. Pembaharuan hukum pidana (*panel reform*) merupakan bagian dari kebijakan / politik hukum pidana (*panel policy*). Makna dan hakikat pembaharuan hukum pidana berkaitan erat dengan latar belakang dan urgensi diadakanya pembaharuan hukum pidana itu sendiri. Latar belakang dan urgensi diadakanya pembaharuan hukum pidana dapat ditinjau dari aspek sosiopolitik, sosiofilosofis, sosiokultural atau dari berbagai aspek kebijakan (khususnya kebijakan sosial, kebijakan kriminal dan kebijakan penegakan hukum). Artinya pembaharuan hukum pidana juga pada hakikatnya harus merupakan perwujudan dari perubahan dan pembaruan terhadap berbagai aspek dan kebijakan yang melatar belakanginya itu. Dengan demikian, pembaruan hukum pidana pada hakikatnya mengandung makna, suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosiopolitik, sosiofilosofis, sosiokultural masyarakat Indonesia yang melandasi kebijakan

¹¹ Henny Nuraeny, *Tindak Pidana Perdagangan Orang, Kebijakan Hukum Pidana dan Pencegahannya*, Sinar Grafik, Jakarta, 2011, hlm. 43,

¹² Lilik Mulyadi, *Pembalikan Beban Pembuktian Tindak Pidana Korupsi*, Alumni, Bandung, 2007, hlm. 62.

1 sosial, kebijakan kriminal dan kebijakan penegakan hukum di Indonesia.¹³

Soejono Soekanto (1988) menyebutkan lima unsur penegakan hukum (*law enforcement*). Artinya untuk mengimplementasikan penegakan hukum di Indonesia ini sangatlah di pengaruhi oleh lima faktor :

- a. Undang-Undang;
- b. Metalitas aparat penegak hukum;
- c. Perilaku Masyarakat (Kesadaran Hukum Masyarakat);
- d. Sarana;
- e. Kultur.

Dalam kelima faktor tersebut terjadi saling mempengaruhi diantara faktor yang satu ke faktor yang lainnya. Eksistensi norma hukum yang berumus didalam undang-undang misalnya sebagai *law in book* sangatlah ditentukan prospeknya ditenagah masyarakat dalam aspek *law in action* atau hukum dalam bangunan realitasnya oleh mentalitas aparat penegak hukum akan menjadi penentu prospek penegakan norma-norma hukum.¹⁴

Faktor-faktor lain yang mempengaruhi penegakan hukum yaitu sarana dan prasarana bantuan hukum, kesejahteraan apart penegak hukum daan kemajuan ilmu pengetahuan teknologi.

“**Satjipto Rahardjo** mengemukakan bahwa penegakan selalu akan melibatkan manusia di dalamnya dan dengan demikian akan melibatkan tingkah laku manusia juga. Hukum tidak dapat tegak dengan sendirinya, artinya hukum tidak mampu mewujudkan janji-janji serta kehendak yang

¹³ Barda Nawawi Arief, *Kebijakan Hukum Pidana*, Kencana Prenada Media Grup, Jakarta, 2008, hlm.22.

¹⁴ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime) Op Cit*, hlm. 136

mencantum dalam (peraturan-peraturan) hukum tersebut. Janji dan kehendak seperti itu, misalnya adalah untuk memberikan hak kepada seseorang, untuk memberikan perlindungan kepada seseorang, untuk mengenakan pidana terhadap seseorang yang memenuhi persyaratan tertentu sebagainya”.

Pada dasarnya setiap orang harus dinyatakan tidak bersalah sebelum ada putusan hakim yang *inkracht* dan *gewijsde*, sehingga merupakan implementasi dari asas *presumption of innocence* atau praduga tidak bersalah. Untuk dapat menyatakan seseorang bersalah, artinya memang benar melakukan kejahatan sebagaimana yang didakwakan terhadapnya, dalam hal ini hukum tentang pembuktian memegang peranan yang sangat penting.

Berdasarkan Pasal 6 Ayat (3) Undang-Undang Nomor 48 Tahun 2009 tentang kekuasaan kehakiman, menyatakan:

“Tiada seorangpun dapat dijatuhi pidana, kecuali apabila Pengadilan karena alat bukti yang sah menurut undang-undang, mendapatkan kenyakinan, bhwu seseorang dianggap bertanggungjawab, telah bersalah atas perbuatan yang dituduhkan atas dirinya.”

3. *Cyberterrorism* .

¹ *Cyberterrorism* merupakan salah satu jenis *Cyber Crime* dari beberapa jenis- jenis *Cyber Crime* yang ada, yang muncul akibat dari dampak negatif perkembangan sarana teknologi informasi dan komunikasi masyarakat global, sehingga terjadi perubahan-perubahan pola perilaku masyarakat dalam bidang ini sebagai penyalahgunaan komputer¹⁵.

¹⁵ Berasal dari computer abuse (Inggris), computermisbruik (Belanda). Lihat dalam Al Wisnubroto hlm 20

Istilah “*Cyberterrorism*” diciptakan untuk penggunaannya berbasis komputer dan serangannya juga terhadap aset-aset musuh. Itu terjadi di dunia maya untuk terrorism berkumpulan (denning 1999). Meskipun serangan ini terjadi di dunia maya, mereka masih menunjukkan empat elemen umum untuk semua aksi terrorism :

- a. Terencana dan bukan sekedar kisah lahir kemarahan serangan *Cyberterrorism* yang premediated dan harus direncanakan sejak mereka melibatkan pengembangan atau *acquistition* perangkat lunak untuk melaksanakan serangan.
- b. Politik dirancang untuk mempengaruhi struktur politik komputer terrorism adalah tindakan yang dimaksudkan untuk merusak atau benar-benar menghancurkan sistem komputer (Galley, 1996). *Cyberterrorism hecker* dengan motivasi politik, serangan mereka dapat mempengaruhi struktur politik melalui korupsi dan kehancuran.
- c. Ditujukan pada warga sipil dan instalasi sipil, serangan *Cyberterrorism* sering mengambil target kepentingan sipil. Denning (2000) memenuhi syarat *Cyberterrorism* sebagai serangan yang mengakibatkan kekerasan terhadap orang atau harta, atau setidak-tidaknya menyebakan kerugian cukup untuk merasakan rasa takut.
- d. Dilakukan oleh kelompok-kelompok *ad hoc* bukan oleh tentara nasional, *Cyberterrorism* kadang-kadang dibedakan dari perang maya atau perang informasi, serangan yang berbasis komputer yang diatur oleh agen-agen berbangsa-bangsa.

Perang maya adalah istilah yang sering digunakan untuk menggambarkan berbagai aspek membela dan menyerang

informasi dan jaringan komputer di dunia maya, serta menolak musuh kemampuan untuk melakukan sama.

Cyber perang dan perang informasi menggunakan teknologi informasi sebagai alat perang untuk menyerang musuh sistem komputer kritis.

Pesatnya perkembangan teknologi informasi yang membawa dampak tumbuh suburnya *Cyber Crime*, kejahatan melalui Internet di jagat maya itu membuat beberapa negara-negara bersepekat melakukan usaha secara bersama-sama dalam menganggulangi tindak pidana *Cyber Crime* tersebut. Usaha-usaha itu terlihat dari pembahasan dalam sidang komisi di Konferensi Ke-23 Aseanapol di Manila, Filipina, September lalu, mengenai *Cyber Crime*, yang diyakini menjadi masalah serius yang harus segera ditangani. Kepolisian di 10 negara Asia Tenggara menyatakan peduli terhadap dampak yang ditimbulkan kejahatan ini dan berupaya untuk menekannya.

Perang informasi pribadi melibatkan serangan berbasis komputer pada data tentang individu. Ini mungkin melibatkan hal-hal seperti mengungkapkan atau merusak informasi rahasia pribadi, seperti medis atau kredit *file*. Perang informasi perusahaan mungkin melibatkan Spionase industri atau menyebarkan informasi keliru tentang pesaing melalui internet. Perang informasi global ditunjukan pada sistem komputer negara yang amat penting. Tujuannya adalah untuk mengacaukan negara dengan mengnonaktifkan sistem, seperti energi, komunikasi atau transportasi.

Tingkat lain komputer bermotif serangan sering disebut sebagai carding kombinasi aktivisme politik dan hacking. Maksud dalam carding akan mengganggu operasi normal tapi tidak menyebabkan kerusakan serius. Ini mungkin termasuk

website instansi pemerintah, banjir email otomatis, dan virus yang lemah. Oleh karena itu, *carding* dibedakan *Cyberterrorism* oleh tingkat kerusakan dan gangguan yang dimaksudkan oleh hacker bermotif politik.

¹ Tak ada satu negara pun yang terbebaskan dari *Cyber Crime*. Perkembangan teknologi telah mengaburkan batas-batas fisik dan budaya sebuah negara. Mengacu pada Kongres Perserikatan Bangsa-Bangsa (PBB) untuk Pencegahan Kejahatan di Wina, Austria, April 2000, *Cyber Crime* meliputi melakukan akses tanpa izin, merusak data atau program komputer, melakukan sabotase untuk menghilangkan sistem atau jaringan komputer, mengambil data dari dan ke dalam jaringan komputer tanpa izin, serta mematai-matai komputer.

Indonesia telah mensahkan salah satu Rancangan Undang-Undang yang berkaitan dengan kejahatan dunia maya (*cybercrime*) yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) diperbaharui menjadi Nomor 19 tahun 2016. Undang-Undang ini bertujuan untuk mengharmonisasikan antara instrumen peraturan hukum nasional dengan instrumen-instrumen hukum internasional yang mengatur teknologi informasi diantaranya, yaitu: *The United Nations Commissions on International Trade Law (UNCITRAL)*, *World Trade Organization (WTO)*, Uni Eropa (EU), APEC, ASEAN, dan OECD.

Masing-masing organisasi mengeluarkan peraturan atau model *law* yang mengisi satu sama lain. Dan juga instrument hukum internasional ini telah diikuti oleh beberapa negara, seperti: Australia (The cyber crime act 2001), Malaysia (Computer Crime Act 1997), Amerika Serikat (Federal legislation:

update April 2002 UNITED STATES CODE), Kongres PBB ke 8 di Havana, Kongres ke X di Wina, kongres XI 2005 di Bangkok, berbicara tentang *The Prevention of Crime and the Treatment of Offender*. Dalam Kongres PBB X tersebut dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan ketentuan yang berhubungan dengan kriminalisasi, pembuktian dan prosedur (*States should seek harmonization of relevant provision on criminalization, evidence, and procedure*) dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya.¹⁶

F. Metode Penelitian.

Metode penelitian adalah tata cara atau prosedur yang digunakan untuk mencairkan kebenaran dan meningkatkan aspek ilmiah. Metode penelitian yang digunakan penulis sebagai berikut:

1. Metode Pendekatan

Metode penelitian yang digunakan dalam penelitian ini adalah metode pendekatan hukum yuridis normatif, artinya pada pokoknya penelitian didasarkan pada data kepustakaan atau data sekunder. Metode pendekatan yuridis normatif yaitu metode pendekatan untuk mencari prinsip-prinsip dasar yuridis, yakni dengan mempelajari dan mengkaji asas-asas hukum, khususnya asas-asas hukum hukum dalam kaidah-kaidah hukum positif yang berasal dari bahan-bahan kepustakaan

¹⁶ Barda Nawawi Arife. *Tindak Pidana Mayantara, Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja Grafindo Persada : Jakarta, hal. v

yang ada, seperti bahan hukum primer berupa peraturan perundang-undangan dan ketentuan lainnya¹⁷

Menurut **Soerjono Soekanto** dan **Sri Mamuji**, penelitian hukum normatif mencakup :

- a. Penelitian terhadap asas-asas hukum;
- b. Penelitian terhadap sistematika hukum;
- c. Penelitian terhadap taraf sinkronisasi vertikal dan horizontal.

2. Spesifikasi Penelitian.

Penelitian yang dilakukan merupakan penelitian deskriptif analisis, yaitu pemberian gambaran umum yang menyeluruh dan sistematika mengenai Penegakan Hukum Terhadap Pelaku Kejahatan *Cyberterrorism* Dihubungkan Dengan Undang-Undang 19 Tahun 2016 Atas Perubahan Undang-Undang No 19 Tahun 2016 Tentang Informasi Transaksi Elektronik.

Gambaran umum tersebut dianalisis dengan berlandaskan pada peraturan perundang-undangan, pendapat ahli serta praktik penerapan hukum tentang *Cyberterrorism* yang ada selama ini, sehingga pada akhirnya bertujuan untuk mencari dan mendapatkan jawaban atas identifikasi masalah yang akan dibahas lebih lanjut.

3. Jenis dan Sumber Data.

Guna memperoleh datang yang mendujung penelitian ini, maka jenis dan sumber data di peroleh melalui:

a. Bahan Hukum Primer

Terdiri dari bahan-bahan hukum yang mengikat yaitu:

- 1) Undang-Undang Dasar 1945;
- 2) Kitab Undang-Undang Hukum Acara Pidana;

¹⁷ Rony Hanitijo Soemitro, *Metode penelitian Hukum dan Jurimetri*, Ghalil Indonesia, jakarta, 1988, hlm.24.

- 3) Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik;
- 4) Undang-Undang teroris

b. Bahan Hukum Sekunder.

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer, seperti rancangan undang-undang, hasil hasil penelitian, hasil karya dari kalangan umum, dan seterusnya sebagai contoh adalah:

- 1) Buku-buku yang menguraikan tentang *Cyber Crime*;
- 2) Buku-buku yang menguraikan tentang Terorisme;
- 3) Buku-buku yang menguraikan Tentang *Cyberterrorism* ;
- 4) Makalah, Jurnal, Ebook, dan berbagai berita di Media Cetak dan Elektronik yang mengulas tentang Penegakan Hukum terhadap pelaku *Cyberterrorism* ;

c. Bahan Hukum Tersier.

Bahan hukum tersier adalah bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus, ensiklopedia, indeks kumulatif dan seterusnya.

Penelitian hukum normatif yang sepenuhnya mempergunakan data sekunder, maka penyusunan kerangka konsepsional mutlak diperlukan, penelitian hukum normatif tidak diperlukan penyusunan atau perumusan jawaban sementara terhadap masalah yang masih bersifat praduga karena masih harus dibuktikan kebenarannya (hipotesa).

Untuk teknik pengecekan data atau pengecekan keabsahan data, dilakukan melalui teknik pemeriksaan triangulasi, khususnya triangulasi sumber, **Patton** dalam

“Qualitative” data analisys; *A sourcebook of new method*”, sebagaimana dikutip oleh **Lexi J Meloeng** yang menyebutkan triangulasi dengan sumber berarti membandingkan dan mengecek balik tingkat kepercayaan suatu yang diperoleh melalui waktu dan alat yang berbeda dalam metode kualitatif.¹⁸

4. Teknik Pengumpulan dan Pengelolaan Data.

Dalam melakukan pengumpulan data, dilakukan melalui penelitian kepustakaan (*Library research*), yaitu dengan mengumpulkan dan mempelajari data sekunder tentang Penegakan Hukum Terhadap Pelaku Kejahatan *Cyberterrorism* Dihubungkan Dengan Undang-Undang 19 Tahun 2016 Atas Perubahan Undang-Undang No 19 Tahun 2016 Tentang Informasi Transaksi Elektronik.

5. Analisi Data.

Setelah beberapa tahapan dalam penelitian ini dilalui, maka pada tahap akhir peneliti ini dilakukan analisis data. Analisis data dilakukan secara kualitatif yaitu suatu cara penelitian yang menghasilkan data deskriptif analisis, tanpa menggunakan angka-angka dari segala sesuatu yang dinyatakan oleh responden secara tertulis atau lisan, dipelajari sebagai sesuatu yang utuh. Dengan kata lain peneliti tidak hanya mengungkapkan kebenaran belaka, tetapi memahami kebenaran tersebut.¹⁹

G. Sistematika Penulisan.

Untuk memberikan materi dan penjelasan yang universal dan sistematis, penulis menyusunnya dalam beberapa bab diantaranya :

¹⁸ Lexi J Meloeng, *Metode Penelitian Kualitatif*, Remaja Rosda karya, Bandung, 2001, hlm.178.

¹⁹ Rony hanitijo, Op Cit, hlm 22.

Bab I. Latar belakang permasalahan, konsep perumusan masalah, kegunaan penelitian, kerangka pemikiran, metode penelitian dan sistematika penyusunan karya ilmiah skripsi

Bab II. Landasan teori yang digunakan dalam pembahasan materi Perkembangan Internet dan *Cyberterrorism*

Bab III. Landasan teori mengenai Tindak Pidana *Cyberterrorism*

Bab IV. Pembahasan secara konseptual mengenai Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyberspace* Sebagai Sarana *Cyberteroris* Dihubungkan Dengan Undang-Undang Tentang Informasi Transaksi Elektronik, dan merupakan inti dari penelitian dan jawaban dari identifikasi masalah.

Bab V. Penutup yang mencangkup simpulan dari rumusan masalah yang termasuk dan saran yang diberikan kepada pihak-pihak terkait.

19%
SIMILARITY INDEX

19%
INTERNET SOURCES

0%
PUBLICATIONS

0%
STUDENT PAPERS

PRIMARY SOURCES

1 www.scribd.com **19%**
Internet Source

Exclude quotes Off

Exclude bibliography Off

Exclude matches < 13%