BAB I

PENDAHULUAN

A. Latar Belakang Penelitian

Kemajuan ilmu pengetahuan dan teknologi membawa berbagai implikasi kompleks dalam kehidupan manusia dan hubungan antar negara. Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan K yang disebut dengan *cyber crime* atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus *cyber crime* di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer.

Adanya *cyber crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet. Beberapa pendapat mengindentikkan *cyber crime* dengan *computer crime*. *The U.S. Department of Justice* memberikan pengertian computer crime sebagai: *"...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".* Pengertian tersebut identik dengan yang diberikan *Organization of European Community Development*, yang mendefinisikan *computer crime* sebagai: *"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".* Adapun Andi Hamzah dalam tulisannya "Aspek-aspek

Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai: "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal". [1] Dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders di Havana*, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal:

1. *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu prilaku ilegal atau melanggar secara langsung menyerang sistem keamanan suatu komputer atau data yang diproses oleh computer.
2. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu perilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa *cyber crime* dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *cyber crime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia informasi dan teknologi khususnya media internet. Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa *hardware/software* maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya.

---

[1] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1990, hlm. 23-24.

Cyber-security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

Global *cyber-security* dibangun di atas 5 (lima) bidang kerja: Global *cyber-security* dibangun di atas 5 (lima) bidang kerja:[2]

1. kepastian Hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak);
2. struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru);
3. kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (undang-undang *cyber crime*);
4. teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak);

[2]Edmon Makarim, *Indonesian Legal Framework for Cybersecurity, http://www.nisc.go.jp/security site/campaign/ ajsympo/pdf/lecture2.pdf,* diunduh pada Kamis 30 Mei 2019, pukul 15. 40 WIB.

5. struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).

Dalam tataran kebijakan, penanganan *cyber crime* berbeda dengan penanganan kejahatan lainnya. Pemerintah umumnya dapat dengan mudah mengendalikan dan menerapkan hukum di dalam wilayah kedaulatan negaranya. Namun tidak demikian terhadap aktivitas-aktivitas *online* yang letak atau lokasinya secara fisik dapat berubah sewaktu-waktu, bahkan hanya dapat dibayangkan.[3]

Pada Tahun 2017 melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara dibentuklah Badan Siber dan Sandi Negara. Tugas Badan Siber Dan Sandi Nasional berdasarkan Pasal 2 Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara, menyatakan bahwa: "Badan Siber Dan Sandi Nasional mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber."

[3] Elizabeth Longworth, *The Possibilities for legal framework for cyberspace- Including New Zealand Perspective*, Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1, Aldershot: Ashgate Publishing Limited, 2000, hlm, 14.

Dengan adanya badan baru yang dibentuk langsung oleh presiden seharusnya memiliki dampak yang signifikan, tetapi yang terjadi malah justru sebaliknya. Kasus kejahatan siber kian meningkat. Menurut laporan dari perusahaan keamanan *Positive Technologies*, pertumbuhan kasus kejahatan siber dari tahun ke tahun mencapai 47 persen jika dibandingkan antara kuartal kedua 2017 dengan kuartal kedua 2018.

Menurut *National Cyber Security Index* (NCSI), bahwa:

> "Sebuah indeks yang disusun untuk mengukur keamanan siber secara global, saat ini Indonesia menempati urutan 105 dari 130 negara yang paling rentan diretas dengan nilai *Security Index* 19,48 poin."[4]

Berdasarkan uraian latar belakang di atas, maka penulis tertarik untuk mengetahui kedudukan Peraturan Presiden dalam menangani kejahatan digital agar terciptanya kepastian hukum, sehingga melakukan penelitian dengan judul skripsi **Kewenangan Badan Siber Dan Sandi Nasional Dalam Menangani Kejahatan Digital *(Cyber Crime)* Berdasarkan Peraturan Presiden No. 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.**

B. Identifikasi Masalah

1. Bagaimanakah kewenangan Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime)* ?

[4] https://indopos.co.id/read/2019/04/15/171847/serangan-siber-ancam-kepentingan-nasional-ini-posisi-indonesia/, diunduh pada Senin 15 April 2019, pukul 14.36 WIB.

2. Apakah yang menjadi hambatan dan upaya Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime)* berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara?

C. Tujuan Penelitian

1. Untuk mengetahui, mengkaji dan menganalisis tentang kewenangan Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime)* berdasarkan Peraturan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.
2. Untuk mengetahui, mengkaji dan menganalisis tentang hambatan dan upaya Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime)* berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

D. Kegunaan Penelitian

Hasil penelitian hukum ini diharapkan dapat memberikan kegunaan secara teoritis maupun praktis, antara lain sebagai berikut:

1. Kegunaan teoritis, menggambarkan kemanfaatkan secara khusus bagi pengembangan ilmu hukum tata negara dan secara umum bermanfaat bagi pengembangan ilmu hukum.

2. Secara praktis, menggambarkan bagaimana manfaat hasil penelitian dalam skripsi ini bagi praktis hukum dan instansi yang terkait dalam bidang hukum tata negara tentang Kewenangan Badan Siber dan Sandi Negara dalam Kejahatan Digital *(Cyber Crime).*

E. Kerangka Pemikiran

Penelitian ini membahas beberapa teori yang akan digunakan untuk menganalisa permasalahan penelitian. Peneliti menggunakan landasan teori yang mendukung pemikiran peneliti tentang teori dan praktik. Peneliti juga menggunakan beberapa teori yang terdiri atas teori negara hukum, teori kewenangan umum, dan teori siber. Pada zaman modern, konsep negara hukum di Eropa Kontinental dikembangkan antara lain oleh Immanuel Kant, Paul Laband, Julius Stahl, Fichte, dan lain-lain dengan menggunakan istilah Jerman, yaitu *rechsstaat*. Hal-hal yang semula tampak tersebar dan berdiri sendiri dapat disatukan dan ditunjukkan kaitannya satu sama lain secara lebih bermakna.[5]

Adapun dalam tradisi Anglo Amerika, konsep negara hukum dikembangkan atas kepeloporan A.V. Dicey dengan sebutan *the rule of law*. Menurut Julius Stahl, konsep Negara Hukum yang disebutnya dengan istilah Rechsstaat itu mencakup empat elemen penting, yaitu:[6]

---

[5] Koentjaraningrat, *Metode-Metode Penelitian Masyarakat*, Gramedia Pustaka Utama, 1997, hlm. 21.

[6] Jimly Asshiddqie, *Konstitusi & Konstitualisme Indonesia*, Cet. 2. Jakarta: Sinar Grafika, 2011, hlm. 125

1. Perlindungan hak asasi manusia;
2. Pembagian kekuasaan;
3. Pemerintahan berdasarkan undang-undang;
4. Peradilan tata usaha negara.

Adapun A.V. Dicey menguraikan adanya tiga ciri penting dalam setiap negara hukum yang disebutnya dengan istilah *The Rule of Law*, yaitu:[7]

1. *supremacy of law*.
2. *equality before the law.*
3. *due process of law.*

Keempat prinsip rechsstaat yang dikembangkan oleh Julius Stahl di atas pada pokoknya dapat digabungkan dengan ketiga prinsip *the rule of law* yang dikembangkan oleh A.V. Dicey untuk menandai ciri-ciri Negara Hukum modern di zaman sekarang. Bahkan, oleh "*The International Commission of Jurists*", prinsip-prinsip negara hukum itu ditambah lagi dengan prinsip peradilan bebas dan tidak memihak (*independence and impartiality of judiciary*) yang pada zaman sekarang makin dirasakan mutlak diperlukan dalam setiap negara demokrasi.[8]

Penjelasan teori negara nukum ini kembali lagi ditegaskan Muhammad Yamin, yang menyatakan Indonesia adalah Negara Hukum (*rechstaat, government of law*) tempat keadilan Hukum tertulis berlaku.[9] Dalam Pasal 1

---

[7] *Ibid*, hlm. 126.
[8] *Ibid*. hlm. 127.
[9] Muhammad Yamin, *Proklamasi dan Konstitusi Republik Indonesia*, Ghalia Indonesia, Jakarta, 1989, hlm. 72.

ayat (3) Undang-Undang Dasar 1945 menyebutkan, bahwa "Negara Indonesia negara hukum." Negara hukum dimaksud adalah negara yang menegakan supermasi hukum yang menegakan kebenaran dan keadilan dan tidak ada kekuasaan yang tidak dipertanggungjawabkan.[10]

Hamid S. Attamimi mengutip Burkens, mengatakan bahwa negara hukum (*rechtstaat*) secara sederhana adalah negara yang menempatkan hukum sebagai dasar kekuasaan negara dan penyelenggaraan kekuasaan tersebut dalam segala bentuknya dilakukan di bawah kekuasaan hukum.[11] Salah satu ciri negara hukum adalah adanya Peradilan Administrasi atau Peradilan Tata Usaha Negara.

Good Governance adalah cita-cita yang menjadi visi setiap penyelenggaraan negara di berbagai belahan bumi, termasuk Indonesia. Secara sederhana *good governance* dapat diartikan sebagai prinsip dalam mengatur pemerintahan yang memungkinkan layanan publiknya efisien dan administrasinya bertanggungajawab pada publik.[12] Menurut Hardijanto, pengertian *governace* mengandung makna yang lebih luas dari pada government, termasuk didalamnya mencakup mekanisme pengelolaan sumber daya ekonomi dan sosial yang melibatkan sektor negara masyarakat dan

---

[10] Majelis Permusyawaratan Rakyat Republik Indonesia, *Makalah Panduan Pemasyarakatan Undang-Undang Dasar Republik Indonesia Tahun 1945*, Sekertaris Jendral MPR RI, Jakarta, 2009, hlm. 46.

[11] Ridwan H.R, *Hukum Administrasi Negara*, Raja Grafindo Persada, Jakarta, 2006, hlm. 87.

[12] Pandji Santosa, *Administrasi Publik Teori dan Aplikasi Good Governance*, Refika Aditama, Bandung, 2008, hlm. 55.

swasta (negara non-negara) sedangkan *goverment* hanya mengacu pada mekanisme suatu pengelolaan berdasarkan kewenangan tertinggi.

Tujuh asas umum penyelenggaraan pemerintahan yang baik (*good governance principles*) menurut Undang-Undang Nomor 28 Tahun 1999 tentang Penyelenggaraan Negara yang Bersih dan Bebas dari Korupsi, Kolusi dan Nepotisme, yaitu:

1. Asas kepastian hukum;
2. Asas Tertib Penyelenggaraan Negara;
3. Asas Kepentingan Umum;
4. Asas Keterbukaan;
5. Asas Proporsionalitas;
6. Asas Profesionalitas; dan
7. Asas Akuntabilitas.

Secara umum, asas tersebut dalam konteks *good governance* dapat disarikan menjadi tiga hal, yaitu; akuntabilitas publik, kepastian hukum, dan transparasi publik.[13]

Fokus kajian *teori kewenangan* adalah berkaitan dengan sumber kewenangan dari pemerintah dalam melakukan perbuatan hukum dalam hubungannya dengan hukum publik maupun dalam hubungannya dengan hukum privat. Pada umumnya negara yang berideologi hukum formal (klasik) mengenal tipe negara liberal individualis kapitalistik, sehingga dalam

[13] *Ibid*, hlm. 56

perwujudannya, negara yang bertipe semacam ini semata-mata bertindak sebagai penjaga malam (*nachtwaschterstaat, Nachwachter*).[14]

Indroharto, mengemukakan tiga macam kewenangan yang bersumber dan peraturan perundang-undangan. Kewenangan itu, meliputi [15]

1. atribusi;
2. delegasi; dan
3. mandat.

Atribusi ialah pemberian kewenangan oleh pembuat undang-undang sendiri kepada suatu organ pemerintahan, baik yang sudah ada maupun yang baru sama sekali. Legislator yang kompeten untuk memberikan atribusi wewenang itu, dibedakan antara:

1. Yang berkedudukan sebagai original legislator di tingkat pusat adalah MPR sebagai pembentuk konstitusi (*konstituante*) dan DPR bersama sama pemerintah sebagai yang melahirkan suatu undang-undang, dan di tingkat daerah adalah DPRD dan pemerintah daerah yang melahirkan peraturan daerah;
2. Yang bertindak sebagai delegated legislator, seperti presiden yang berdasarkan pada suatu ketentuan undang-undang mengeluarkan peraturan pemerintah di mana diciptakan wewenang-wewenang pemerintahan kepada Badan atau Jabatan TUN tertentu.

---

[14] E. Utrecht, *Pengantar Hukum Administrasi Negara*, Ichtiar Baru, Jakarta, 1985, hlm. 3-4.

[15] Ridwan HR., *Hukum Administrasi Negara*, Raja Grafindo Persada, Jakarta, 2006, hlm. 104.

Delegasi adalah penyerahan wewenang yang dipunyai oleh organ pemerintahan kepada organ yang lain. Dalam delegasi mengandung suatu penyerahan, yaitu apa yang semula kewenangan si A, untuk selanjutnya menjadi kewenangan si B. *Black Law Dictionary* dikenal istilah *"theory of law* yaitu *the legal premise or set of principles on which a case rest.*[16] dalam bahasa Belanda dikenal dengan istilah *"leer"* yang berarti ajaran pokok, yaitu pendapat yang dikemukakan sebagai keterangan mengenai suatu peristiwa atau kejadian, atau dapat pula berarti asas dan hukum umum yang menjadi dasar suatu kesenian atau ilmu pengetahuan.[17] Kewenangan yang telah diberikan oleh pemberi delegasi selanjutnya menjadi tanggung jawab penerima wewenang. Mandat, di situ tidak terjadi suatu pemberian wewenang baru maupun pelimpahan wewenang dan Badan atau Pejabat TUN yang satu kepada yang lain. Tanggung jawab kewenangan atas dasar mandat masih tetap pada pemberi mandat, tidak beralih kepada penerima mandat.

F.A,M. Stroink dan J.G. Steenbeek, seperti dikutip oleh Ridwan HR, mengemukakan bahwa dua cara organ pemerintah memperoleh kewenangan, yaitu: [18]

1. atribusi; dan
2. delegasi.

---

[16] Bryan A.Gadamer (ed), *Blacks Law Dictionary*, West Publishing.Co.Min, St. Paul, 1999, hlm. 1517.

[17] Marjane Termorshuisen, *Kamus Hukum Belanda-Indonesia*, Djambatan, Jakarta, 2002, hlm. 209.

[18] Ridwan HR., *op.cit*, hlm. 105.

Atribusi berkenaan dengan penyerahan wewenang baru, sedangkan delegasi menyangkut pelimpahan wewenang yang telah ada (oleh organ yang telah memperoieh wewenang secara atributif kepada organ lain; jadi secara logis selalu didahului oleh atribusi). Kedua cara organ pemerintah dalam memperoleh kewenangan itu, dijadikan dasar atau teori untuk menganalisis kewenangan dari aparatur negara di dalam menjalankan kewenangannya. Philipus M. Hadjon membagi cara memperoleh wewenang atas dua cara, yaitu:[19]

1. atribusi; dan
2. delegasi dan kadang-kadang juga mandat.

Atribusi merupakan wewenang untuk membuat keputusan (*besluit*) yang langsung bersumber kepada undang-undang dalam arti materiil. Atribusi juga dikatakan sebagai suatu cara normal untuk memperoleh wewenang pemerintahan. Sehingga tampak jelas bahwa kewenangan yang didapat melalui atribusi oleh organ pemerintah adalah kewenangan asli, karena kewenangan itu diperoleh langsung dari peraturan perundang-undangan (utamanya UUD 1945). Dengan kata lain, atribusi berarti timbulnya kewenangan baru yang sebelumnya kewenangan itu, tidak dimiliki oleh organ pemerintah yang bersangkutan. Delegasi diartikan sebagai penyerahan wewenang untuk membuat *besluit* oleh pejabat pemerintahan (pejabat Tata Usaha Negara) kepada pihak lain tersebut. Dengan kata penyerahan, ini berarti

[19] Philipus M. Hadjon, 1998, *Wewenang Pemerintahan (bestuurbevoegdheid*), Pro Justitia, Vol. XVI N. I, hlm. 90.

adanya perpindahan tanggung jawab dan yang memberi delegasi (*delegans*) kepada yang menerima delegasi (*delegetaris)*. Suatu delegasi harus memenuhi syarat-syarat tertentu, antara lain:[20]

1. Delegasi harus definitif, artinya delegans tidak dapat lagi menggunakan sendiri wewenang yang telah dilimpahkan itu;
2. Delegasi harus berdasarkan ketentuan peraturan perundang-undangan, artinya delegasi hanya dimungkinkan kalau ada ketentuan untuk itu dalam peraturan perundang-undangan;
3. Delegasi tidak kepada bawahan, artinya dalam hubungan hierarki kepegawaian tidak diperkenankan adanya delegasi;
4. Kewajiban memberi keterangan (penjelasan), artinya delegasi berwenang untuk meminta penjelasan tentang peiaksanaan wewenang tersebut;
5. Peraturan kebijakan (*beleidsregel*) artinya delegasi memberikan instruksi (petunjuk) tentang penggunaan wewenang tersebut.

Mandat diartikan suatu pelimpahan wewenang kepada bawahan. Pelimpahari itu bermaksud memberi wewenang kepada bawahan untuk membuat keputusan a/n pejabat Tata Usaha Negara yang memberi mandat. Pada delegasi terjadilah pelimpahan suatu wewenang yang telah ada oleh Badan atau Jabatan TUN yang telah memperoleh suatu wewenang pemerintahan secara atributif kepada Badan atau Jabatan TUN lainnya. Jadi, suatu delegasi selalu didahului oleh adanya sesuatu atribusi wewenang. Pada

[20] Philipus M. Hadjon, 1998, *Wewenang Pemerintahan (bestuurbevoegdheid*), Pro Justitia, Vol. XVI N. I, hIm. 94.

mandat, disitu tidak terjadi suatu pemberian wewenang baru maupun pelimpahan wewenang dari Badan atau Jabatan TUN yang satu kepada yang lain.[21]

Tanggungjawab tidak berpindah ke mandataris, melainkan tanggungjawab tetap berada di tangan pemberi mandat, hal ini dapat dilihat dan kata a.n (atas nama). Dengan demikian, semua akibat hukum yang ditimbulkan oleh adanya keputusan yang dikeluarkan oleh mandataris adalah tanggung jawab si pemberi mandat. Sebagai suatu konsep hukum publik, wewenang terdiri atas sekurang-kurangnya tiga komponen, yaitu :[22]

1. pengaruh;
2. dasar hukum; dan
3. konformitas hukum.

Komponen pengaruh ialah bahwa penggunaan wewenang dimaksudkan untuk mengendalikan perilaku subjek hukum. Komponen dasar hukum ialah bahwa wewenang itu selalu harus dapat ditunjuk dasar hukumnya dan komponen konformitas hukum mengandung makna adanya standar wewenang, yaitu standar umum (semua jenis wewenang) dan standar khusus (untuk jenis wewenang tertentu). Kaitannya di Indonesia, penerapan hukum siber dan efektivitasnya sebagaisuatu tataran norma yang berfungsi sebagai

---

[21] Indroharto, *Usaha Memahami Undang-undang tentang Peradilan Tata Usaha Negara*, Pustaka Harapan, Jakarta, 1993, hlm. 68.

[22] *Ibid*, hlm. 90.

penanggulangan isu-isu yang tadi sudahsecara singkat disebutkan dapat dikaji melalui pendapat Friedman.[23]

Menurut Hasyim Gautama, kerangka hukum *cyber-security* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 sertasurat edaran menteri dan peraturan menteri.[24]

Ini berdampak pada terdapat kekosongan hukum mengenai pengaturan *cyber crime* yang kian luas jenisnya. Secara umum, dalam tulisannya, Hamid Jahankhani (*et.al*.) mengkategorikan *cyber crime* menjadi:[25] *Phising, Spam, Cyber Harrassment or Bullying, Identity Theft, Plastic Card Fraud*, dan *Internet Auction Fraud.* Ditambah lagi, masih banyak masyarakat yang belum begitumemahami aturan-aturan atau hukum yang menyangkut *cyber crime*, sehinggaterkadang masih ada masyarakat yang menilai *cyber crime* bukanlah masalah yang terlalu serius untuk dibahas.[26]

Definisi konvensional *cybersecurity* yang dapat ditemukan di berbagai strategi pemerintah maupun buku panduan perusahaan adalah sesuatu yang terkait dengan perlindungan informasi yang terdapat di dalam lingkungan

---

[23] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, disadur oleh Pent. M.Khozim, Nusamedia, Bandung, 2011, hlm. 18.

[24] Handrini Ardiyanti, 2014, *Cyber-Security dan Tantangan Pengembangannya di Indonesia*", Politica, Vol. 5 No. 1, hlm. 100.

[25] Hamid Jahankhani (*et.al*.), 2014, *Cybercrime classification and characteristics*, dalam: Babak Akhgar (eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook,* Waltham: Elsevier, hlm. 159-160.

[26] Widi Nugrahaningsih dan Indah Wahyu Utami, 2014, *Implementasi Penyelesaian Cybercrime* dengan Dasar Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di Kota Surakarta, *GEMA*, Vol. 26 No. 48, hlm.1427.

digital dari penyusupan, akuisisi maupun eksploitasi tanpa izin. Meskipun demikian, *cybersecurity* telah memiliki makna yang jauh lebih luas. Pemerintah, lembaga, media dan masyarakat sipil sama-sama menggunakan istilah ini untuk merujuk berbagai hal dalam konteks yang lebih luas. Hal-hal di bawah ini dapat dianggap sebagai beberapa contoh isu dalam *cybersecurity*:

1. Suatu serangan phishing menyebabkan jebolnya data *log-in* akun bank banyak orang; Kelemahan piranti lunak yang membuat private *key server*, cookies serta password pengguna mudah dijebol;
2. Sistem keamanan informasi rumah sakit yang lemah dan menghambat akses data pasien; *malware* yang menyebabkan padamnya lampu di satu kota;
3. Kelompok teroris merencanakan serangan melalui jaringan tersembunyi;
4. Pasokan air suatu kota menjadi tidak aman ketika seorang *hacker* mengambil alih kendali secara remote dari sebuah instalasi air;
5. Sebuah video yang melanggar hak cipta diunggah ke sebuah website; Suatu jaringan pengedar narkoba menggunakan *crypto-currency* untuk memperdagangkan narkotika ilegal;
6. Sebuah komentar yang menghina seorang pemimpin politik diposting di suatu jaringan sosial media.

Istilah *cyber security* juga dapat dijadikan alasan untuk menerapkan kebijakan yang dapat melanggar hak asasi manusia (HAM). Misalnya, *cyber security* seringkali digunakan oleh sejumlah negara untuk membenarkan

pembatasan *browsing* internet secara tidak transparan dan akuntabel, melarang penggunaan aplikasi anonimitas dan layanan enkripsi, serta memperluas kewenangan aparat penegak hukum untuk melakukan pengintaian tanpa berpedoman pada kebijakan dan tata laksana yang memadai, proporsional, dan profesional. Ruang siber (*cyberspace*) adalah ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya intenet) untuk melakukan berbagai kegiatan sehari-hari.[27] Dalam kajian Strategis Keamanan Siber Nasional, mendefinisikan ancaman kejahatan siber *(cyber crime)* sebagai setiap kondisi dan situasi serta kemampuan yang dinilai dapat melakukan tindakan atau gangguan atau serangan yang mampu merusak atau segala sesuatu yang merugikan sehingga mengancam kerahasiaan *(confidentiality),* integritas *(integrity),* dan ketersedian *(availability)* sistem dan informasi.[28]

Dibandingkan dengan berbagai isu kebijakan lain yang dapat berdampak pada HAM, *cyber security* menghadapi tantangan konseptual yang berbeda. Hal ini antara lain disebabkan dari sifat "keamanan" (*security*) itu sendiri. Keamanan tidak akan pernah dapat dicapai seratus persen atau secara sempurna. Karena itu, *cyber security* masih berada pada posisi yang terus berubah dan dapat dibentuk dan dibangun oleh pengampu kebijakan majemuk (*multistake holder*). Keberagaman multistake holder yang terlibat dalam *cyber security* juga memberikan tantangan tersendiri. Ini merupakan isu bagi

[27] Kementerian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, Kemhan RI, Jakarta, 2014, hlm.5.

[28] Iwan, *Kajian Strategi Keamanan Cyber Nasional*: *Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber*, Tesis Universitas Pertahanan Indonesia, Jakarta, 2012.

pemerintah, lembaga antar pemerintah, komunitas teknis dan akademisi, sektor swasta serta masyarakat sipil. Dengan belum adanya definisi yang ajeg, istilah *cybersecurity* ini menjadi amat luas, dan digunakan untuk merujuk hal seperti serangan siber (*cyber attack*) hingga spam, dan bahkan standar teknis sistem pemungutan suara (*voting*).

Jika kita memandang keamanan sebagai kebebasan dari bahaya atau ancaman, salah satu pendorong terpenting dalam pembuatan kebijakan *cyber security* adalah bagaimana ancaman dipahami dalam *cyberspace*. Tanpa upaya *cyber security* yang tepat, kemungkinan ancaman akan meningkat. Secara umum ancaman dipandang mencakup hal-hal berikut:

1. Pencurian data untuk keuntungan komersial, seperti pencurian nomor kartu kredit, atau pencurian data pribadi untuk digunakan untuk spamming atau pencurian identitas;
2. Akses kepada data untuk kepentingan mata-mata industri demi mendapatkan keunggulan kompetitif;
3. Pencurian data untuk menghancurkan nama baik, atau mendiskreditkan pemerintah atau suatu entitas bisnis, serta mendiskreditkan orang atau sekelompok orang;
4. Mengakses data untuk mengumpulkan data intelijen yang dilakukan oleh negara asing maupun entitas non-negara;
5. Pengubahan atau penghapusan data untuk alasan komersial, politik, maupun ekonomi;

6. Kehilangan kendali atas jaringan akibat serangan yang dirancang untuk melemahkan atau melumpuhkan pemerintah atau suatu perusahaan;
7. Manipulasi perilaku pengguna dengan cara memancing pengguna mengunduh (download) malware atau tanpa sengaja melakukan tindakan membahayakan diri lainnya;
8. Ancaman kepada karyawan atau publik dengan melakukan serangan siber untuk melumpuhkan fungsi lembaga publik tertentu.

Meskipun masih belum ada kesepakatan tentang istilah yang digunakan dan isu yang akan dihadapi,sejumlah upaya telah dilakukan selama ini untuk mengatasi ancaman-ancaman yang disebutkan di atas, yang mencakup antara lain:

1. Upaya teknis untuk meningkatkan keamanan peragkat keras *(hardware)* dan piranti lunak *(software)* yang mencakup sistem dan jaringan informasi. Hal ini dilakukan antara lain dengan menguji sistem yang bersangkutan dengan standar teknis yang ada seperti teknik kriptografi, manajemen identitas dan akses, manajemen risiko rantai pasokan serta jaminan atas kehandalaan *software*;
2. Upaya hukum juga memainkan peranan dalam mengatur persyaratan untuk mendapatkan, menyimpan, memproses serta membagi informasi pribadi oleh lembaga swasta maupun publik. Upaya hukum yang relevan mencakup hukum perlindungan data;

3. Upaya terkait proses yang mencakup prosedur, panduan, keputusan institusi dan materi pendidikan yang dirancang untuk meminimalkan peran orang- yang terpisah dari komputer dalam menciptakan atau memfasilitasi gangguan *cyber* seperti melalui serangan rekayasa sosial maupun kebiasaaan penggunaan password yang lemah.

Dengan pertimbangan bahwa bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional, pemerintah memandang perlu dibentuk badan dengan menata Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara, guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber. Atas dasar pertimbangan tersebut, pada 19 Mei 2017, Presiden Jokowi telah menandatangani Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Tugas Badan Siber dan Sandi Negara adalah membangun ekosistem ranah siber Indonesia yang kuat dan aman. Selain itu Badan Siber dan Sandi Negara juga menjadi penyelenggara dan pembina persandian Negara dalam menjamin keamanan informasi, utamanya yang berklasifikasi milik pemerintah atau negara, dengan tujuan untuk menjaga keamanan nasional. Badan Siber dan Sandi Negara berfungsi untuk mendeteksi, mencegah, dan menjaga keamanan siber mengingat banyak aksi-aksi kejahatan yang memanfaatkan dunia maya dalam beberapa waktu ke belakang.

Secara spesifik, fungsi Badan Siber dan Sandi Negara antara lain:

1. Identifikasi, deteksi, proteksi, dan penanggulangan *e-Commerce.*
2. Persandian.
3. Diplomasi siber.
4. Pusat manajemen krisis siber.
5. Pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber.

Membasmi hoaks yang banyak beredar di dunia maya juga termasuk dalam fungsi Badan Siber dan Sandi Negara. Lebih luas lagi, fungsi Badan Siber dan Sandi Negara mencakup pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi. Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembvangan teknologi informasi yang begitu cepat untuk lebih mendalam ada beberapa pendapat dibawah ini tentang apa yang dimaksud dengan *cyber crime*? Diantaranya adalah menurut kepolisisan Inggris, *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal/atau kriminal berteknologi tinggi dengan mneyalah gunakan kemudahan teknologi digital.[29] Dalam dua dokumen kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention Of Crime And Treatment Of Offenders* di Havana kuba pada tahun 1990 dan di Wina

[29] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* PT. Rafika Aditama, Jakarta, 2005, hlm. 40.

Austria pada tahun 2000, menjelaskan ada dua istilah yang terkait dengan *Cyber Crime* yaitu *Cyber Crime* dan *computer related crime*.[30]

Badan Siber dan Sandi Negara berperan dalam mengawal Indonesia memasuki era ekonomi digital (*e-Commerce*), big data, dan *fintech*, yang selalu dibayangiserangan siber. Menkominfo Rudiantara menegaskan, untuk menjaga kesinambungan keamanan siber dan informasi nasional, maka ID-SIRTII tetap menjalankan tugasnya di Kominfo hingga siap dilaksanakan oleh Badan Siber dan Sandi Negara, jika Badan Siber dan Sandi Negara sudah memiliki anggaran dan struktur organisasinya. Program Jangka Panjang Badan Siber dan Sandi Negara adalah memberikan perlindungan kepada masyarakat Warga Negara Indonesia (WNI) di samping tugas mengamankan instansi pemerintah, BUMN, dan sektor swasta dengan batasan peraturan untuk dapat memenuhi harapan Presiden Jokowi. Badan Siber dan Sandi Negara dirancang dengan model kolaborasi antara pemerintah, swasta, akademisi, beserta masyarakat, dengan doktrin pertahanan defensif, melakukan fungsi perlindungan, deteksi dini, prefentif (pencegahan), identifikasi, penanggulangan, dan *recovery* (restorasi/pemulihan). *Cyber crime* atau kejahatan dunia maya adalah kejahatan yang dilakukan oleh seseorang maupun kelompok yang menguasai dan mampu mengoperasikan komputer

[30] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penagnggulangan Kejahatan,* Kencana Perdana Media Group, Jakarta, 2007, hlm. 24.

dan alat telekomunikasi lainnya. Cara-cara yang biasa yang dilakukan dengan merusak data, mencuri data dan menggunakannya secara ilegal.[31]

F. Metode Penelitian

Metode penelitian ini dimaksudkan, untuk dapat mengetahui, dan membahas suatu permasalahan, maka diperlukan adanya pendekatan dengan menggunakan metode tertentu, yang bersifat ilmiah. Metode menurut Arief Subyantoro dan FX Suwarto yang dikutip dari buku Anthon F. Susanto, metode adalah prosedur atau cara untuk mengetahui sesuatu dengan langkah-langkah sistematis. [32]

1. Spesifikasi Penelitian

Penelitian ini menggunakan spesifikasi penelitian yang bersifat deskriptif analitis yang memberikan data atau gambaran seteliti mungkin mengenai objek permasalahan. Spesifikasi penelitian yang bersifat deskriptif analitis menurut Soerjono Soekanto, yaitu: enggambarkan fakta-fakta hukum dan atau peraturan perundang-undangan yang berlaku secara komprehensif mengenai objek penelitian untuk kemudian dikaitkan dengan teori-teori hukum dalam praktik pelaksaannya yang menyangkut permasalahan yang diteliti. [33]

2. Metode Pendekatan

---

[31] Abdul Wahib dan Mohammad Labib, *op.cit*, hlm 15

[32] Anthon F. Susanto, *Penelitian Hukum Transformatif-Partisipatoris Fondasi Penelitian Kolaboratif Dan Aplikasi Campuran (Mix Method) Dalam Penelitian Hukum*, Setara Press, Malang, 2015, hlm.159-160.

[33] Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1986, hlm. 10.

Metode pendekatan yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif. Ronny Hanitijo Soemitro, menyatakan bahwa: "pendekatan yuridis normatif, yaitu penelitian dalam bidang hukum yang dikonsepsikan terhadap asas-asas, norma-norma, dogma-dogma atau kaidah-kaidah hukum yang merupakan patokan tingkah laku dalam penelitian ini dilakukan dengan cara mengkaji ketentuan perundang-undangan dengan tetap mengarah kepada permasalahan yang ada sekaligus meneliti implementasinya dalam praktik". [34] Metode penelitian dengan pendekatan yuridis normatif ini diperlukan, karena data yang digunakan adalah data sekunder dengan menitik beratkan.

Penelitian pada data kepustakaan yang diperoleh melalui penelusuran bahan-bahan dari buku, literatur, artikel, jurnal, dan situs internet yang berhubungan dengan hukum atau aturan yang berlaku khususnya yang berkaitan dengan Badan Siber dan Sandi Negara dalam kajahatan digital *(cyber crime)*.

3. Tahap Penelitian

Tahap penelitian ini dilakukan dalam dua tahap yang bertujuan untuk memudahkan penulis dalam pengolahan data, yaitu:

a. Penelitian Kepustakaan (*Library Research*)

---

[34] Ronny Hanitijo Soemintro, *Metode Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990, hlm. 5.

1) Bahan-bahan hukum primer, yaitu bahan-bahan hukum yang mengikat, terdiri dari beberapa peraturan perundang-undangan sebagai berikut:
   a) Undang-Undang Dasar 1945.
   b) Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia
   c) Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.
   d) Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara.
2) Bahan hukum sekunder, yaitu bahan yang memberikan penjelasan mengenai bahan hukum primer, yang terdiri dari buku-buku, makalah, hasil-hasil penelitian yang berkaitan dengan penelitian ini dan artikel dari surat kabar serta internet.
3) Bahan hukum tersier, yaitu bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap hukum primer dan sekunder, seperti kamus hukum, dan kamus besar bahasa Indonesia.

b. Penelitian Lapangan (*field research*)

> Menurut Soerjono Soekanto, penelitian lapangan ialah: Penelitian lapangan yaitu suatu cara untuk memperoleh data yang dilakukan dengan mengadakan observasi untuk

mendapatkan keterangan-keterangan yang akan diolah dan dikaji berdasarkan peraturan yang berlaku.[35]

Penelitian ini dilakukan secara langsung terhadap objek penelitian dan dimaksudkan untuk memperoleh data yang bersifat data primer sebagai penunjang data sekunder.

4. Teknik Pengumpulan Data

Data Pada penelitian ini, akan diteliti data primer dan data sekunder. Dengan demikian ada dua kegiatan utama yang akan dilakukan dalam penelitian ini, yaitu studi kepustakaan *(library research)* dan studi lapangan *(field research).* Penulis akan mengumpulkan data dengan cara studi dokumen, yaitu mencari data-data selengkap mungkin dari data sekunder yang berasal dari bahan-bahan primer, sekunder, dan tersier, dan didukung dengan data dari lapangan. Data sekunder diperoleh melalui studi kepustakaan dengan mengkaji, menelaah, dan mengelola literatur, peraturan perundang-undangan, artikel-artikel, jurnal-jurnal dan tulisan yang berkaitan dengan permasalahan ini.

a. Studi kepustakaan *(library research)*

Studi kepustakaan yaitu suatu metode yang mempelajari dan meneliti literatur tentang hal-hal yang berhubungan dengan Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime)*

b. Studi Lapangan (*Field Reseacrh*)

[35] Soerjono Soekanto, *op.cit,* hlm. 11.

Selain dengan menggunakan studi kepustakaan, dalam penelitian itu, peneliti juga menggunakan data lapangan untuk memperoleh data yang bersifat primer sebagai penunjang data sekunder dilakukan dengan cara mencari data di lokasi atau objek penelitian serta mengadakan wawancara dengan pihak Badan Siber dan Sandi Negara ataupun dengan pihak Kepolisian Republik Indonesia yang terkait tentang kejahatan digital *(cyber crime).*

5. Alat Pengumpul Data

Penelitian ini dilakukan dengan cara mencari dan mengumpulkan data baik dari perundang-undangan, wawancara, internet maupun buku-buku yang berhubungan dengan Badan Siber dan Sandi Negara dalam menangani kejahatan digital *(cyber crime).* Alat yang dipergunakan oleh peneliti dalam memperoleh data sebagai berikut :

a. Data Kepustakaan

1) Menggunakan catatan untuk memperoleh data yang dilakukan secara tertulis.
2) Menggunakan laptop dalam memperoleh data yang diperoleh dari alamat website internet.
3) Menggunakan flashdisk sebagai penyimpan data yang diperoleh dari alamat website internet atau dari narasumber.

b. Wawancara

Wawancara dilakukan oleh penulis kepada pihak Badan Siber

dan Sandi Negara serta kepada pihak Kepolisian Republik Indonesia terkait kejahatan digital *(cyber crime).*

6. Analisis Data

Teknik yang dipakai penulis untuk menganalisis data yang dikumpulkan yaitu dengan metode yuridis kualitatif. Penggunaan yuridis kualitatif yaitu karena dalam penelitian ini data akan dianalisis secara kualitatif yaitu dengan disajikan secara deskriptif yang menggambarkan permasalahan secara menyeluruh.

7. Lokasi Penelitian

a. Studi Kepustakaan

1) Perpustakaan Fakultas Hukum Universitas Pasundan Bandung, Jalan Lengkong Besar Dalam No.17, Bandung;

2) Perpustakaan Fakultas Hukum Universitas Padjajaran, Jalan Dipatiukur No.35, Bandung.

b. Studi Lapangan

Badan Siber dan Sandi Negara (BSSN), Jl. Raya Muchtar No.70, Bojongsari Lama, Kec.Bojongsari, Kota Depok, Jawa Barat 16516.