

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan sistem teknologi informasi dan elektronik dalam sebuah negara merupakan hal yang paling utama dalam menjalankan prinsip kedaulatan negara. Negara dikatakan berdaulat apabila keamanan dalam sistem teknologi dan informasi nya dapat di lindungi dan dijaga keamanan serta kerahasiannya dari berbagai ancaman. Untuk mewujudkan cita-cita dan tujuan bernegara membutuhkan penyelenggara negara. Penyelenggara negara yang dimaksud yakni pemerintah. Pemerintah merupakan bagaian dari alat negara yang melaksanakan tugas (fungsi)".¹ Pemerintah dalam hal ini perlu membentuk suatu lembaga negara/alat negara yang dapat bertanggung jawab dalam keamanan dan kedaulatan negara khususnya di bidang sistem teknologi informasi dan elektronik.

Lembaga negara yang dimaksud menurut pendapat Padmo Wahjono, yakni "alat perlengkapan suatu negara yang memiliki peran mendasar dalam kegiatan suatu kenegaraan".² Dengan hadir dan banyaknya lembaga negara atau alat negara dalam pengamanan di bidang digital/siber, diharapkan mampu memberikan kontribusi yang optimal dalam tanggung jawab kepada negara di bidang pengamanan siber. Namun yang terjadi sebaliknya banyaknya lembaga negara/organ negara yang ada menjadi dilematis dalam implementasi praktik di

¹ C.S.T. Kansil, *Sistem Pemerintahan Indonesia*, (Jakarta : Aksara Baru, 1983), hlm.21.

² Padmo Wahjono, *Beberapa Masalah Ketatanegaraan Di Indonesia*, (Jakarta : CV. Rajawali, 1984), hlm. 17.

dalam ketatanegaraan karena sering terjadi adanya tumpang tindih wewenang tanggung jawab antar lembaga negara yang ada. Di dalam beberapa kasus kejahatan khususnya di bidang siber ini, lembaga negara yang ada saling lempar melempar suatu tanggung jawab.

Kasus yang baru-baru ini viral dalam kejahatan di bidang siber yakni munculnya *Hacker Bjorka* yang menamai dirinya sebagai “*Bjorka*”³

“kasus *Hacker Bjorka* ini menjadi perhatian publik karena yang ia lakukan meretas sejumlah data pemerintah serta melakukan *doxing* terhadap beberapa pejabat publik, kemudian ia juga menyebarkan sejumlah data pribadi milik pejabat publik yang termuat nama, Nomor Induk Kependudukan (NIK), dan Kartu Keluarga (KK) sampai alamat rumah”.

Bahwa tindakan yang dilakukan oleh *Hacker Bjorka* ini adalah tindakan kejahatan siber. “Untuk menangani kejahatan dalam siber (*cybercrime*) membutuhkan adanya hukum siber (*cyber*) atau yang dikenal dengan nama *cyber law*”.⁴ di Indonesia sendiri sudah ada aturan yang mengatur mengenai tentang kejahatan siber.

Lahir dan adanya Undang-Undang Informasi Dan Transaksi elektronik (UU ITE) merupakan bagaian upaya memberantas kejahatan khususnya dalam bidang teknologi dan informasi. “Saat ini Undang-Undang No. 19 Tahun 2016 (UU ITE) menjadi tolak ukur dalam penindakan kejahatan yang ada dalam sosial media, yang mana ini merupakan bagian dari kemajuan hukum dalam untuk menuntaskan

³ Edi Saputra Hasibuan, Lia Salsiah, “Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia”, *Jurnal Pro Hukum*, Vol. 11 No. 3 Oktober 2022.

⁴ Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime Di Indonesia*, (Jakarta : Raja Grafindo Persada, 2006).

persoalan-persoalan yang belum bisa dapat diselesaikan dengan baik”.⁵ Selain itu juga dengan adanya Undang-Undang No. 27 Tahun 2022 tentang perlindungan data pribadi, adanya pengakuan dan penghormatan atas pentingnya perlindungan data pribadi seseorang, agar hak warga negara terhadap perlindungan diri pribadinya dapat terlindungi dan terjaga dari beberapa kejahatan yang ada khususnya di dalam media sosial.

Pemerintah sebagai penyelenggara negara dalam hal ini sudah membentuk organ/alat negara dalam pengamanan di dunia digital/siber yang mana kurang lebih ada 4 (empat) lembaga negara yang berkaitan dengan pengamanan di ruang siber. Yakni Badan Siber dan Sandi Negara (BSSN), Menteri Komunikasi dan Informasi (MENKOMINFO), *Virtual Police*/Polisi Siber, dan Badan Intelijen Negara (BIN). Kesemuanya lembaga negara atau organ negara ini masing-masing mempunyai dasar hukum sendiri-sendiri yang mengatur. BSSN dibentuk oleh Presiden dengan dasar hukum pembentukan Perpres No 28 Tahun 2021, MENKOMINFO dengan dasar hukum Perpres 54 Tahun 2015, *Virtual Police*/Polisi Siber dengan dasar hukum SE Kapolri bernomor SE/2/11/2021 dan BIN dengan dasar hukum pembentukan Perpres No. 73 Tahun 2017.

BSSN merupakan lembaga negara yang bertanggung jawab langsung kepada Presiden untuk melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi dalam rangka membantu Presiden untuk menyelenggarakan urusan pemerintahan. Hal ini jelas dalam ketentuan Pasal 15 huruf (c) Peraturan Presiden

⁵ Sherly Nelsa Fitri, “Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia”, *Jurnal Justisia*, Vol. 7 No.1 2022, hlm. 121.

No. 28 Tahun 2021 fungsi dari Deputi II yang berbunyi “*Menyelenggarakan fungsi pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang indentifikasi, deteksi proteksi, penanggulangan, pemulihan, dan pemantauan insiden keamanan siber dan sandi nasional, serta pengelolaan krisis siber nasional*”.⁶ Jika dikaitkan dalam persoalan tanggung jawab negara dalam hal kasus *Hacker Bjorka* BSSN juga menjadi bagaian yang turut bertanggung jawab dalam kasus kejahatan ini.

Selain itu lembaga negara yang juga memiliki keterkaitan dengan keamanan di ruang digital/siber yakni MENKOMINFO. Dalam ketentuan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan sistem dan transaksi elektronik menjelaskan PSE bertanggung jawab untuk urusan sistem keamanan di platformnya. Dalam Pasal 1 angka 3 PP No.71 Tahun 2019 PSE adalah “*setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain*”.⁷ Al hasil, “Menkominfo mempunyai tanggung jawab dalam mengurus data-data yang dikelolanya, selain korporasi juga memegang data pelanggannya sendiri”.⁸

⁶ Lihat Peraturan Presiden Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara Pada Pasal (15).

⁷ Lihat Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggara Sistem Elektronik (PSE) Pada pasal (1) angka 3.

⁸ <https://www.cnnindonesia.com/teknologi/20220916032811-192-848550/siapa-tanggung-jawab-urus-bocor-data-seperti-kasus-bjorka/2>. (diakses pada tanggal 6 November 2022).

Selain itu ada juga *Virtual Police* unit yang dibentuk melalui Surat Edaran KAPOLRI dibawah satuan *Cyber* Badan Reserse Kriminal, juga memiliki keterkaitan dengan keamanan siber. Bahwa Surat Edaran tersebut menjelaskan bahwa POLRI bertujuan untuk “mengedepankan edukasi serta langkah persuasif terhadap masyarakat yang memposting atau menyampaikan sesuatu bersifat melanggar hukum, sehingga diharapkan bisa menghindari adanya dugaan kriminalisasi serta menciptakan ruang digital Indonesia agar tetap bersih, sehat dan produktif”.⁹ Sehingga dalam hal ini menjadi pertanyaan sejauh mana peran *Virtual Police* dalam menanggulangi atau memberantas kasus kejahatan siber *Hacker Bjorka* ini, yang mana *Hacker Bjorka* ini menyebarkan data pribadi seseorang dan juga banyak sekali membocorkan data terkait dengan arsip kenegaraan sehingga menyebabkan ruang digital menjadi tidak sehat.

Berikutnya yakni ada Badan Intilijen Negara dengan dasar hukum pembentukan Perpres No.73 Tahun 2017 “memiliki Deputy Bidang Intilijen Siber (*Cyber*) dalam struktur BIN”.¹⁰ Dalam melaksanakan tugas di bidang intilijen siber Pasal 25C berbunyi “Dalam melaksanakan tugasnya sebagaimana dimaksud dalam ketentuan Pasal 25B, “Deputi VI Menyelenggarakan fungsi :

⁹ Rahardian Satya Mandala Putra dkk, “Pembentukan Virtual Police Dari Perspektif Ham Di Indonesia”, *Jurnal Hukum Lex Generalis*, Vol.2. No.8 (Agustus 2021).

¹⁰ Surwandono dkk, “Menakar Paradigma Keamanan Nasional Melalui Analisis Isi Terhadap Undang-Undang No. 17 Tahun 2011 Tentang Intelijen Negara”, *Jurnal Mandala*, Vol. 1 No.1 Januari – Juni 2018, hlm. 34.

- a. Penyusunan rencana kegiatan dan/atau operasi intilijen siber;
- b. Pelaksanaan kegiatan dan/atau operasi intilijen siber
- c. Pengkoordinasian kegiatan dan/atau operasi intilijen siber: dan
- d. Menyusun laporan intilijen siber”.¹¹

Jika melihat pada ketentuan yang ada dalam Pasal 25 B pada huruf (b) maka BIN juga seharusnya memiliki keterkaitan tanggung jawab dalam menjaga keamanan negara di ruang siber pada kasus *Hacker Bjorka* ini.

Pemerintah sebagai penyelenggara negara mempunyai peran penting di dalam menjaga kedaulatan negara. Dalam pembukaan Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD NRI 1945), memberikan amanat bahwa tujuan negara adalah untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Adanya Undang-Undang No.27 Tahun 2022 tentang perlindungan data pribadi memberikan amanah kepada badan publik “Pemerintah” dalam menyelenggarakan perlindungan data pribadi. Maka Lembaga negara yang ada harus turut ikut dalam menjaga keamanan dalam perlindungan data dan ancaman keamanan siber nasional. Sehingga dalam hal ini menarik untuk dibahas dalam skripsi yang berjudul “TINJAUAN YURIDIS TANGGUNG JAWAB NEGARA DALAM MENJAGA KEAMANAN SIBER PADA KASUS *HACKER BJORKA* DI INDONESIA”.

¹¹ Lihat Peraturan Presiden Nomor 73 Tahun 2017 Tentang Badan Intelijen Negara, Pada Pasal 28B.

1.2 Rumusan Masalah

Setelah melihat pada uraian latar belakang masalah diatas maka dengan ini dapat diambil rumusan masalah sebagai berikut :

- a. Mengapa terjadi tumpang tindih kewenangan dalam penanganan *Hacker* ?
- b. Bagaimana penataan Lembaga Negara yang berwenang dalam menjaga keamanan siber ?

1.3 Tujuan

Adapun tujuan dari penelitian dalam skripsi ini yakni sebagai berikut :

- a. Untuk mengetahui mengapa terjadi tumpang tindih kewenangan dalam penanganan kasus *Hacker Bjorka*
- b. Untuk menganalisis bagaimana penataan Lembaga Negara dalam menjaga keamanan di ruang digital dan siber nasional.

1.4 Kegunaan

Adapun kegunaan dari penelitian dalam skripsi ini yakni sebagai berikut :

- a. Secara Teoritis

Secara teoritis penelitian ini diharapkan dapat menemukan konsep baru terkait dengan kewenangan dalam penanganan kasus *Hacker* dan bagaimana Penataan Kelembagaan Negara dalam menangani kasus *Hacker*.

b. Secara Praktis

Adapun kegunaan secara praktis dari penulisan karya tulis ilmiah ini diharapkan dapat mampu memberikan pemahaman dan pemikiran baru kepada negara khususnya dalam penanganan dibidang siber nasional serta memberikan pemahaman terhadap penataan kelembagaan yang ada terkait dalam praktik ketatanegaraan dalam menjaga keamanan digital/siber nasional.

1.5 Keaslian Penelitian

Dalam karya tulis ilmiah hukum ini dengan judul “Tinjauan Yuridis Tanggung Jawab Negara Dalam Menjaga Keamanan Siber Pada Kasus *Hacker Bjorka* Di Indonesia” adalah asli sesuai dengan ide gagasan dan pemikiran oleh penulis. Sebagai pembandingan dapat dikemukakan dari hasil penelitian oleh beberapa peneliti sebagai berikut :

- a. Novi Nour Hidayati dengan Judul Skripsi “Tinjauan Fiqh Siyasah terhadap penagulangan kejahatan digital berdasarkan Peraturan Presiden Nomor 133 tahun 2017 perubahan atas Peraturan Presiden Nomor 53 tahun 2017”. Penelitian ini menitikberatkan pada kewenangan Badan Siber Dan Sandi Negara serta hambatan-hambatan BSSN dalam menanggulangi serangan siber baik dari prespektif hukum positif maupun dalam fiqh siyasah.

- b. Topan Syahid Cahyadin dengan judul Skripsi “Kewenangan Badan Siber Dan Sandi Negara Dalam Menangani Kejahatan Digital (*Cyber Crime*) Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara”. Penelitian ini menitikberatkan pada kewenangan BSSN dalam Menangulangi Kejahatan di ruang Digital (*Cyber Crime*) berdasarkan ketentuan PerPres Nomor 53 Tahun 2017. Hasil penelitian menunjukan penanganan *Cyber Crime* dapat melaksanakan kerjasama terhadap penyidik aparat kepolisian ataupun PPNS, Kominfo dan dalam hal upaya penangulangan seragan kejahatan siber yakni infrastruktur teknologi yang belum merata, regulasi yang masih tumpang tindih, bergantung pada produk impor dan minimnya kualitas serta kuantitas sumber daya manusia nya.

Untuk mempermudah mengetahui penelitian sebelumnya dengan penelitian yang akan penulis lakukan, berikut disajikan dalam tabel 1 memperlihatkan mengenai keaslian dan orsinalitas penelitian dan korelasinya serta yang menjadi pembeda dengan hasil penelitian sebelumnya, sebagaimana dibawah ini.

Tabel 1 : Keaslian Penelitian

No	Nama	Judul/asal Fakultas	Fokus Pembahasan	Korelasi Dan Yang Menjadi Pembeda
1	Novi Nour Hidayati	Tinjauan Fiqih Siyasah terhadap penagulangan kejahatan digital berdasarkan Peraturan Presiden Nomor 133 tahun 2017 perubahan atas Peraturan Presiden Nomor 53 tahun 2017. UIN Sunan Ampel Surabaya, 2022.	Tulisan skripsi ini membahas mengenai tentang permasalahan mengenai bagaimana kewenangan Badan Siber Dan Sandi Negara serta hambatan-hambatan BSSN dalam menanggulangi serangan siber baik dari prespektif hukum positif maupun dalam fiqh siyasah.	Penelitian ini memiliki korelasi yakni sama-sama membahas mengenai tentang kejahatan siber, namun yang menjadi pembeda yakni penelitian ini melakukan tinjauan dari sudut Fiqih Siyasah. Dan hanya berfokus pada satu lembaga saja. Sedangkan dalam penelitian penulis membahas mengenai tumpang tindih kewenangan dalam penanganan <i>Hacker</i> dan terkait dengan bagaimana penataan kelembagaan dalam menjaga keamanan siber.

2	Topan Syahid Cahyadin	Kewenangan Badan Siber Dan Sandi Negara Dalam Menangani Kejahatan Digital (<i>Cyber Crime</i>) Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara. Fakultas Hukum Unpas.	Dalam penelitian ini yang menjadi pokok bahasan adalah kewenangan BSSN dalam Menanggulangi Kejahatan di ruang Digital (<i>Cyber Crime</i>) berdasarkan PerPres Nomor 53 Tahun 2017. Hasil penelitian menunjukan penanganan <i>Cyber Crime</i> dapat melaksanakan kerjasama terhadap penyidik aparat kepolisian ataupun PPNS Kominfo dan dalam hal upaya penanggulangan serangan kejahatan siber yakni infrastruktur teknologi yang belum merata, regulasi yang masih tumpang tindih, bergantung pada produk impor dan minimnya kualitas serta kuantitas sumber daya manusia nya.	Penelitian ini memiliki korelasi, yakni sama-sama membahas mengenai penanggulangan kejahatan Digital (<i>Cyber Crime</i>) namun yang menjadi pembeda yakni penelitian ini hanya berfokus pada pembahasan satu lembaga saja yakni BSSN yang diamanati oleh undang-undang. Sedangkan dalam penelitian penulis membahas mengenai tumpang tindih kewenangan dalam penanganan <i>Hacker</i> dan terkait dengan bagaimana penataan kelembagaan dalam menjaga keamanan siber.
---	-----------------------	---	--	--

Sumber : Kreasi Penulis.

1.6 Metode Penelitian

a. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif (*legal research*) atau penelitian hukum doktrinal, karena “penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum”.¹² Penelitian ini disebut juga sebagai penelitian kepustakaan atau studi dokumen maka penelitian ini dilakukan lebih banyak menggunakan data yang bersifat sekunder yang ada di perpustakaan.

b. Pendekatan Penelitian

Pendekatan Penelitian yang digunakan dalam hal ini menggunakan metode pendekatan *statute approach* (pendekatan undang-undang) dengan “menelaah semua peraturan per undang-undangan dan regulasi yang ada dan terkait dengan isu hukum yang sedang di bahas (diteliti)”.¹³ Selain itu juga menggunakan metode pendekatan *conseptual approach* (pendekatan konseptual) “pendekatan ini beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum”.¹⁴

c. Sumber Bahan Hukum

c.1. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang terdiri dari peraturan per undang-undangan, putusan pengadilan dan dokumen

¹² Muhaimin, *Metode Penelitian Hukum*, (Mataram : University Pers, 2020), hlm. 45.

¹³ *Ibid.* hlm. 56.

¹⁴ *Ibid.* hlm. 57.

resmi negara. Dalam penelitian ini menggunakan bahan hukum primer sebagai berikut :

- a). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- b). Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251 dan Tambahan Lembaran Negara Republik Indonesia Nomor 5952).
- c). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan data pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 dan Tambahan Lembaran Negara Republik Indonesia Nomor 6820).
- d). Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.
- e). Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi Dan Informasi (MENKOMINFO).
- f). Peraturan Presiden Nomor 73 Tahun 2017 tentang Badan Intelijen Negara (BIN).
- g). Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber Dan Sandi Negara (BSSN).
- h). Surat Edaran Kapolri bernomor SE/2/11/2021 Tentang Pembentukan *Virtual Police*.
- i). Dan peraturan lainnya yang mendukung penelitian ini.

c.2. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan hukum pendukung untuk pengkayaan dan penguatan terkait dengan bahan hukum primer seperti “pendapat-pendapat para ahli hukum yang termuat dalam buku, karya ilmiah jurnal, artikel dan jenis-jenis tulisan lainnya”.¹⁵ yang berkaitan dengan tanggung jawab negara dalam menjaga keamanan siber di ruang digital nasional.

d. Teknik Pengumpulan Bahan Hukum

Didalam penelitian hukum normatif teknik pengumpulan bahan hukum dengan mengkaji peraturan per undang-undangan yang berkaitan dengan isu hukum yang di hadapi, maka bahan-bahan hukum dengan menggunakan bahan hukum primer dan bahan hukum sekunder.

e. Analisa Bahan Hukum

Analisis Bahan Hukum yang di gunakan dalam penelitian ini bersifat Preskripsi yaitu untuk memberikan argumentasi atas hasil penelitian yang dilakukan. “Argumentasi dilakukan untuk menilai mengenai benar atau salah atau apa yang seyogyanya atau seharusnya menurut hukum, (norma hukum, asas dan prinsip hukum)”.¹⁶ Analisis dilakukan sebagai kegiatan memberikan telaahan yang dapat berarti menentang, atau memberikan komentar dan kemudian membuat suatu kesimpulan terhadap hasil

¹⁵ *Ibid.* hlm. 63.

¹⁶ *Ibid.* hlm. 71.

penelitian dengan menggunakan pikiran sendiri dan dengan bantuan teori yang telah digunakan.

1.7 Sistematika Penulisan

Untuk menghasilkan karya tulis ilmiah yang baik dan untuk mempermudah dalam melakukan pembahasan maka diberikan gambaran besar terkait dengan sistematika penulisan yang terdiri dari 4 (empat) bab dan setiap bab terdiri dari beberapa sub bab yang menyajikan materi yang di bahas.

Adapaun sistematika penulisan skripsi ini sebagai berikut :

BAB I PENDAHULUAN

1.1 Latar Belakang

1.2 Rumusan Masalah

1.3 Tujuan

1.4 Manfaat/Kegunaan

1.5 Metode Penelitian

1.6 Sistematika Penulisan

BAB II KAJIAN PUSTAKA TANGGUNG JAWAB NEGARA DALAM MENJAGA KEAMANAN SIBER

2.1 Pengertian Tanggung Jawab Negara

2.2 Pengertian Keamanan Siber

2.3 Teori Tanggung Jawab

2.4 Teori Perlindungan Hukum

2.5 Teori Kepastian Hukum

BAB III TUMPANG TINDIH KEWENANGAN DAN PENATAAN KELEMBAGAAN

3.1 Tumpang Tindih Kewenangan Dalam Penanganan *Hacker*

3.2 Penataan Lembaga Negara Yang Berwenang Dalam Menjaga Keamanan Siber

BAB IV PENUTUP

4.1 Simpulan

4.2 Saran