BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada era sekarang ini, terdapat peralihan aktivitas manusia dari budaya konvensional menjadi komputasi dan internet sentris.[1] Hal ini dapat di tunjukkan melalui data World Bank yang menyatakan bahwa 60 persen dari populasi dunia telah menggunakan Internet.[2] Data dari *International Telecommunication Union* (ITU) juga membuktikan bahwa semenjak pandemik Corona *Virus* Disease 2019 (COVID-19) angka penggunaan internet mengalami kenaikan sebesar sembilan persen pada tahun 2021, yang sebelumnya berada di angka 54 persen dari total populasi dunia pada tahun 2019 menjadi 63 persen dari total populasi dunia pada tahun 2021.[3] Di Indonesia sendiri, merujuk pada data World Bank mengenai konsumsi internet masyarakat, mengalami kenaikan dari tahun 2019 yang berada di 48 persen menjadi 56 persen pada tahun 2020. Peralihan tersebut dapat di contohkan dalam beberapa bukti, antara lain penggunaan ojek online, pengiriman barang, serta aplikasi kencan online. Hal ini tidak terlepas dari manfaat, efektivitas, dan efisiensi yang diberikan oleh teknologi.[4] Oleh karenanya, Data dan faktatersebut membuktikan bahwa kini manusia dihadapkan oleh dua kehidupan

[1] Kartini Eliva Angel Tampubolon, "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare", *Jurist-Diction*, Vol. 2 No. 2, 2019, hlm. 539 https://doi.org/10.20473/jd.v2i2.14250.

[2] World Bank, "Individuals using the Internet (% of population)", 2022 https://data.worldbank.org/indicator/IT.NET.USER.ZS, diakses 5 September 2022.

[3] International Telecommunication Union, "Internet uptake has accelerated during the pandemic", https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/, diakses pada 5 September 2022.

[4] *Kartini Eliva Angel Tampubolon*, *Loc.Cit.* hlm. 540.

yakni kehidupan dunia nyata dan dunia maya atau yang dikenal dengan nama *cyberspace*.

Cyberspace itu sendiri pertama kali diperkenalkan oleh William Gibson dalam novelnya yakni "*Neuromancer*" pada tahun 1980, ia menyebutkan sebagai berikut:

> *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding...*[5]

Hal ini berkesusaian dengan pendapat Anne Meredith Fulton bahwa *cyberspace* memiliki cakupan yakni seluruh pesan elektronik dan sistem informasi.[6] Lebih lanjut, merujuk pada pendapat Kuehl yang menyatakan bahwa *cyberspace* merupakan domain di dalam lingkungan informasi yang memiliki keunikan dan perbedaan karakter yang dibentuk oleh penggunaan elektronik dan spektrum elektronik untuk menciptakan, menyimpan, memodifikasi, melakukan tukar menukar, dan mengeksploitasi informasi melalui jaringan bebas dan terkoneksi menggunakan teknologi informasi dan komunikasi.[7] Pendapat ahli tersebut di perkuat oleh *US Department of Defense* yang menjabarkan bahwa dunia siber merupakan hubungan antara dimensi fisik dan informasi, yang mencakupi antara lain sistem informasi, jaringan, komputer dan komunikasi, serta infrastruktur

[5] William Gibson, *Neuromancer*, 1984, hlm. 128.
[6] AM Fulton, "Cyberspace and the Internet: Who Will be the Privacy Police", *CommLaw Conspectus: Journal of Communications Law and Policy*, Vol. 3 1995, hlm. 63.
[7] Franklin D. Kramer, Stuart H. Starr, dan Larry K. Wentz, "Cyber Power and National Security", *National Defense University Press*, 2009, hlm. 28.

pendukung.[8] Oleh karenanya, perpindahan ini menciptakan realitas baru yang sebelumnya hanya bersifat nyata menjadi ada yang bersifat maya (*Virtual*), hal ini tidak menutup kemungkinan mengenai kejahatan, salah satunya dibuktikan dengan terciptanya kejahatan khusus siber yakni *cyber threat atau* ancaman siber.

Ancaman siber ini pada dasarnya ialah suatu aktivitas penyerangan terhadap teknologi komunikasi dan informasi dengan menggunakan komposisi komputasi yang di lakukan oleh pelaku tindakan tersebut.[9] Di samping itu, merujuk pada pendapat dalam buku "*Guide to Cyber Threat Information Sharing*" dikatakan bahwa ancaman siber merupakan suatu kejadian yang berpotensi memiliki dampak terhadap operasi organisasi, aset organisasi, perorangan, atau negara melalui sistem informasi dengan cara akses, destruksi, pengungkapan, atau modifikasi informasi, dan pengrusakan pelayanan yang ilegal.[10] Ancaman siber ini juga memiliki beberapa metode yang digunakan, antara lain *Malware*, *Man-in-the-Middle Attacks* dan *Formjacking*, tergantung pada tujuan serta keahlian dari para pelaku ancaman siber tersebut.[11]

Oleh karenanya, tercipta pula metode pengamanan untuk menghindari ataupun memitigasi resiko anacaman tersebut, yakni dikenal dengan *Cybersecurity* atau keamanan siber. Metode keamanan siber ini pada dasarnya ialah suatu organisasi dan koleksi dari sumber, proses, dan struktur yang digunakan untuk

[8] US Secretary of Defense, "The National Military Strategy for Cyberspace Operations", 2006, hlm. 5.

[9] B. A. Obotivere dan A. O. Nwaezeigwe, "Cyber Security Threats on the Internet and Possible Solutions", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 9 No. 9, 2020, hlm. 92 https://ijarcce.com/wp-content/uploads/2020/10/IJARCCE.2020.9913.pdf, diakses 14 Oktober 2022.

[10] Chris Johnson et al., *Guide to Cyber Threat Information Sharing*, National Institute of Standards and Technology, 2016, hlm. 2.

[11] *B. A. Obotivere* dan *A. O. Nwaezeigwe*, *Loc.Cit*. hlm. 94-96.

melindungi ruang siber atau sistem siber dari kejadian yang tidak berkesesuaian dengan *de jure* dan *de facto* hak properti.[12] Sistem keamanan siber ini pula tidak terlepas dari statistik kejahatan siber yang mulai meningkat secara signifikan. Merujuk pada data yang di lansir dari Purplesec, bahwa kejahatan siber meningkat 600% dikarenakan pandemik COVID-19 serta kerugian yang dialami dapat mencapai 6 triliun dolar per tahun dari seluruh dunia.[13] Di Indonesia sendiri, merujuk pada data BSSN, terdapat total 714.170.967 anomali trafik atau serangan siber sepanjang tahun 2022, dengan rincian 279.962.734 kasus terjadi pada bulan januari, pada bulan februari 111 juta serang dan sisanya terjadi pada bulan-bulan selanjutnya.[14]

Salah satu peristiwa yang menggemparkan pun terjadi di Indonesia, yakni penyerangan yang dilakukan oleh *Bjorka*. Dalam aksinya tersebut, ia juga telah melakukan beberapa kali penyerangan siber terhadap aplikasi dan website korporasi dan pemerintah Indonesia, antara lain pembobolan bank data Tokopedia pada tahun 2020,[15] dan pembobolan sistem kementerian komunikasi dan informasi mengenai 1,3 Juta data pengguna kartu SIM[16]. data surat rahasia yang dikirimkan oleh

[12] Dan Craigen, Nadia Diakun-Thibault, dan Randy Purse, "Defining Cybersecurity", *Technology Innovation Management Review*, 2014, hlm. 17.

[13] Purplesec, "The Cost Of Cybercrime", *Purplesec*, Purplesec, 2022 https://purplesec.us/resources/cyber-security-statistics/#:~:text=The global annual cost of,than it was in 2015, diakses 2022.

[14] CNN Indonesia, "RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan", *CNN Indonesia*, https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan, diakses 2022.

[15] CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual", *CNN Indonesia*, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual, diakses 2022.

[16] Kompas.com, "1,3 Miliar Data SIM Card Diduga Bocor, Begini Respons 3 Opsel dan Kominfo", *Kompas.com*, https://tekno.kompas.com/read/2022/09/02/10200017/1-3-miliar-data-sim-card-diduga-bocor-begini-respons-3-opsel-dan-kominfo?page=all, diakses September 2022.

lembaga Badan Intelijen Negara (BIN) kepada Presiden Republik Indonesia, Joko Widodo, selama periode 2019-2020 mengalami kebocoran disebabkan oleh ulah *Bjorka* tersebut.[17] Yang terakhir, bahwa *Bjorka* melakukan peretasan dan membocorkan serta menjual data milik Komisi Pemilihan Umum (KPU) yang mencapai 105 juta data, data tersebut di tampilkan di situs Breached.to dan di jual dengan harga US$5.000.[18] Walaupun begitu, Polisi Republik Indonesia (POLRI) telah menetapkan tersangka MAH sebagai pembantu *Bjorka* dalam melaksanakan aktivitas peretasan tersebut.[19]

Di Indonesia sendiri pada dasarnya memiliki peraturan mengenai sistem informasi baru diundangkan pada tahun 2008 melalui Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam UU ITE tersebut serta perubahannya belum mengatur secara spesifik mengenai ancaman siber serta ketahanan siber sebagaimana yang terjadi sebagai salah satu ancaman besar pada masa kini, walaupun RUU Perlindungan Data Pribadi (RUU PDP) sudah di sahkan menjadi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) akan tetapi tetap tidak dapat mengakomodir konteks ancaman siber yang luas objeknya.

[17] Eqqi Syahputra, "Ancaman Itu Nyata! *Bjorka* Bongkar Dokumen Rahasia Jokowi", *CNBC Indonesia*, https://www.cnbcindonesia.com/tech/20220910072431-37-370881/ancaman-itu-nyata-*Bjorka*-bongkar-dokumen-rahasia-jokowi, diakses 2022.

[18] Lenny Septiani, "Ahli IT: 105 Juta Data KPU 'Dagangan' Hacker *Bjorka* Valid", *Katadata.com*, https://katadata.co.id/desysetyowati/digital/631ac18111474/ahli-it-105-juta-data-kpu-dagangan-hacker-*Bjorka*-valid, diakses 2022.

[19] Sugeng Harianto, "Pemuda Madiun Tersangka Kasus *Bjorka* yang Sempat Menghilang Akhirnya Pulang", *detikJatim*, https://www.detik.com/jatim/berita/d-6296654/pemuda-madiun-tersangka-kasus-*Bjorka*-yang-sempat-menghilang-akhirnya-pulang, diakses September 2022.

Seharusnya UU ITE dapat mengakomodir kepentingan dan perlindungan terhadap layanan siber apabila terjadi ancaman siber tersebut. Sayangnya, di dalam UU ITE itu sendiri hanya mengatur mengenai kejahatan konvensional dalam KUHP yang di lakukan dalam lingkup siber sebagaimana yang tertuang dalam Pasal 27-36 UU ITE. Adapun dalam ketentuan pidana pada UU ITE terkait ancaman siber hanya diatur dalam 4 pasal, yakni pasal 30-33. Oleh karenanya, kualifikasi dalam pasal-pasal tersebut cenderung luas dan misinterpretasi. Padahal di beberapa negara telah memiliki regulasi mengenai ancaman siber antara lain Thailand melalui *Cyber Security Maintenance Act*, yang pada pasal 60 dari peraturan tersebut menjabarkan kualifikasi ancaman siber, dan Vietnam melalui *Law on Cyberinformation Security*, yang menjabarkan mekanisme preventif dan mitigasi terjadinya Malware serta hal tersebut di kualifikasikan menjadi tindak pidana dalam Pasal 7 Ayat 4 pada peraturan tersebut. Di samping itu, problematik mengenai problematika UU ITE juga bertambah setelah diundangkannya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (UU No. 1 Tahun 2023) yang mencabut ketentuan dalam Pasal 30 UU ITE sehingga berpotensi terdapat kekosongan hukum untuk kasus-kasus yang terjadi sebelum UU No. 1 Tahun 2023 tersebut berlaku, salah satunya kasus *Bjorka* yang belum dilakukan proses Pro Justitia sampai dengan saat ini.

Dengan demikian, merujuk pada latar belakang tersebut, penelitian ini akan melakukan analisis yuridis normatif guna menentukan kualifikasi *cyber threat*, dalam hal ini kasus *Bjorka*, sebagai tindak pidana merujuk pada UU ITE. Di samping itu, penelitian ini akan mengakomodir pembahasan mengenai potensi

kekosongan hukum setelah UU No. 1 Tahun 2023 berlaku, yakni 3 tahun sejak undang-undang tersebut diundangkan. Lalu, penelitian ini juga akan mendalami pola pertanggung jawaban pidana terkait dengan studi kasus *Bjorka* dengan kemungkinan bahwa *Bjorka* merupakan sebuah korporasi, pereorangan atau *Artificial Intelligence* (*AI*) sehingga dapat menentukan bentuk pertanggung jawaban pidana terkait objek penelitian tersebut.

1.2. Rumusan Masasalah

1. Apakah *cyber threat* yang dilakukan *Bjorka* memenuhi kualifikasi sebagai tindak pidana ditinjau dari UU ITE?
2. Bagaimana pertanggung jawaban pidana bagi *Bjorka* sebagai pelaku tindak pidana *cyber threat* merujuk pada UU ITE?

1.3. Tujuan Penelitian

1. Melakukan analisis terhadap kualifikasi *cyber threat* sebagai sebuah tindak pidana dalam UU ITE.
2. Menentukan bentuk pertanggung jawaban pidana bagi pelaku *cyber threat* sebagaimana yang diatur dalam UU ITE.

1.4. Manfaat Penelitian

1.4.1. Manfaat Praktis

Hasil penelitian dalam skripsi ini ditujukan untuk penyesuaian kualifikasi tindak pidana UU ITE dengan fenomena terbaru yang terjadi di dalam kehidupan sosial sehingga memberikan kepastian hukum terkait suatu kejadian yang baru.

1.4.2. Manfaat Teoritis

Hasil penelitian dalam skripsi ini ditujukan untuk memberikan penjabaran konseptual, karakteristik, serta akibat dari *cyber threat* sehingga dapat dikualifikasikan sebagai tindak pidana dalam UU ITE.

1.5. Metode Penelitian

1.5.1. Tipe Penelitian Hukum

Tipe penilitian hukum ini akan berdasarkan pada penilitian yang bersifat yuridis normatif. Dalam hal ini merujuk pada pendapat Peter Mahmud Marzuki menyatakan bahwa penelitian hukum normatif merupakan suatu proses guna menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum untuk menjawab isu hukum yang dihadapi.[20] Oleh karenanya dalam penelitian ini akan menggunakan data primer yang berdasarkan pada peraturan perundang-undangan dan sumber hukum lainnya. Di samping itu, penelitian ini akan menggunakan data sekunder seperti buku, jurnal, dan dokumen tambahan lainnya.

[20] Peter Mahmud Marzuki, '*Penelitian Hukum'*, Kencana Prenada Group, 2017, hlm. 35.

1.5.2. Pendekatan Masalah

Penulisan penilitian skripsi menggunakan dua cara pendekatan, yakni pendekatan perundang-undangan (*Statute Approach*), pendekatan secara konspetual (*conceptual approach*), dan studi kasus (*case study*). Merujuk pada pendapat Prof. Peter Mahmud Marzuki, bahwa pendekatan perundang-undangan merupakan pendekatan yang berdasarkan pada penggunaan legislasi dan regulasi.[21] Di samping itu, mengenai pendekatan konseptual merupakan pendekatan yang mengandalkan kajian terhadap konsep terkait ancaman siber yang ditekankan pada metode, tata cara, serta objek penyerangan sehingga dapat dikualifikasikan sebagai tindak pidana dalam UU ITE. Oleh karenanya, melalui pendekatan ini akan merumuskan bahwa ketentuan sebagaimana yang telah diatur dalam UU ITE dapat dikenakan terhadap situasi ancaman siber.

Serta, penelitian ini juga akan menggunakan pendekatan studi kasus (*case study*) yang merupakan pendekatan yang menganalisis kejadian-kejadian serupa mengenai ancaman siber untuk dihubungkan sebagai acuan dalam menentukan bahwa peraturan perundang-undangan di Indonesia dapat berlaku.

1.5.3. Sumber Bahan Hukum

Penelitian ini akan menggunakan bahan hukum yang bersumber pada, yakni:

a. Bahan hukum primer yang terdiri atas peraturan perundang-undangan sebagaimana yang tercantum dalam Undang-Undang Nomor 12 Tahu 2011 tentang Pembentukan Peraturan Perundang-Undangan, yakni:

[21] Peter Mahmud Marzuki, *Penelitian Hukum*, Prenada Media, 2005, hlm. 237.

1. Undang-Undang Republik Indonesia Nomor 1 Tahun 1946 tentang Peratran Hukum Pidana untuk Selurh Wilayah Republik Indonesia dan mengbah Kitab Undang-Undang Hukum Pidana (Wetboek van Strafrecht) Staatsblad Nomor 7322 Tahun 1915 (Lembaran Negara Repblik Indonesia Tahun 1958 Nomor 127, Tambahan Lembaran Negara Republik Indonesia Nomor 1660).
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).
3. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).
4. Undang-Undang Republik Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).
5. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tenntang Pennyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400).

6. Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana Korporasi (Berita Negara Tahun 2016 Nomor 2058).
7. Peraturan Jaksa Agung Nomor PER-028/A/JA/10/2014 tentang Pedoman Penanganan Perkara Pidana dengan subjek Hukum Korporasi (Berita Negara Tahun 2014 Nomor 1492).
8. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Tahun 2002 Nomor 1375).

b. Bahan hukum sekunder yang terdiri atas artikel jurnal, buku, dan dokumen lainnya terkait dengan penelitian ini.

1.5.4. Prosedur Pengumpulan Bahan Hukum

Dalam prosedur pengumpulan bahan hukum, penulis menggunakan prosedur penelitian berdasarkan pada pendekatan statuta dan pendekatan konsep untuk menjawab isu hukum yang terjadi. Oleh karenanya, penulis mengumpulkan bahan hukum berdasarkan peraturan perundang-undangan atau aturan terkait. Lalu, setelah melakukan analisis terhadap perundang-undangan, guna memperkuat argumentasi, maka penulis akan melakukan analisis buku, jurnal, atau dokumen lainnya yang berkaitan dengan jawaban dari isu hukum yang ditemukan.

1.5.5. Analisis Bahan Hukum

Dalam proses analisis bahan hukum, penulis akan melakukan filterisasi mengenai peraturan yang berkaitan dengan isu hukum. Filterisasi ini akan mengupas tuntas unsur-unsur hukum terkait isu hukum yang muncul, yaitu isi pasal terkait yang akan dihubungkan dengan konteks penelitian. Dengan demikian, penulis dapat menyimpulkan hubungan antara peraturan perundang-undangan dengan isu hukum yang terjadi.

1.5.6. Sistematika Penulisan

Pertama, dalam bab pertama penulis akan mendeskripsikan latar belakang masalah yang terjadi terkait isu hukum terkait, menentukan rumusan masalah, menjabarkan mengenai tujuan dan manfaat penelitian, metode penelitian, hingga tujuan pustaka. Informasi tersebut digunakan sebagai basis penelitian yang selanjutnya akan secara jelas dan rinci di bahas dalam bagian pembahasan.

Kedua, pada bab kedua ini, penulis akan menjabarkan mengenai rumusan masalah pertama yakni kualifikasi ancaman siber, dimulai dari metode ancaman siber, subyek hukum, dan peraturan terkait, sebagai tindak pidana merujuk pada UU ITE. Bab ini akan membuka argumentasi penulis perihal hubungan antara ancaman siber dengan UU ITE sebagai tindak pidana yang telah di atur dalam undang-undang tersebut. Pada akhirnya, penulis akan memberikan konklusi mengenai hubungan tersebut.

Ketiga, pada bab ketiga ini, penulis akan menjelaskan mengenai rumusan masalah kedua yakni pertanggung jawaban pidana pelaku ancaman siber. Hal

tersebut akan di dasarkan pada sistematika pertanggung jawaban pidana dalam UU ITE. Selain itu, penulis akan membedah kemungkinan pertanggung jawaban akan di bebankan pada seseorang sesuai ketentuan UU ITE yang berlaku serta melihat asas yang terkait dengan permasalahan tersebut.

Keempat, dalam bab keempat, penulis akan memberikan konklusi dan rekomendasi mengenai isu hukum terkait. Konklusi dan rekomendasi tersebut akan didasarkan pada hasil penelitian dalam bab kedua dan keti