BAB I

PENDAHULUAN

1.1. Latar Belakang

Indonesia merupakan negara dengan penduduk yang memiliki berbagai jenis suku ras dan Bahasa. Negara Indonesia merupakan negara hukum yang sebagaimana diterangkan di dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945, yang berbunyi "Negara Indonesia adalah negara hukum", yang di mana artinya negara adalah pemegang kekuasaan hukum tertinggi untuk menegakan kebenaran dan keadilan, serta tidak ada kekuasaan yang tidak dipertanggungjawabkan."Saat ini dunia dalam kondisi yang lazim disebut globalisasi, dimana hubungan antar subyek seolah-olah tanpa batas (*borderless*)".[1]

Globalisasi saat ini didukung oleh kemajuan teknologi dan informasi yang sangat pesat dengan Sumber Daya Manusia (SDM) yang semakin kreatif demi untuk memenuhi kebutuhan yang semakin kompleks. Untuk menghubungi kolega yang jaraknya beribu-ribu kilo meter cukup dengan tekan angka-angka yang ada pada *handphone*, untuk berdagang dengan mitra bisnis yang berbeda benua juga tidak perlu repot dengan datang ke lokasi yang dimaksud, cukup menggunakan fasilitas perdagangan elektronik (*e-commerce*). "Untuk melakukan aktivitas perbankan juga tidak perlu datang ke bank, cukup memanfaatkan kecanggihan

[1] Tim Dosen Fakultas Hukum Universitas Brawijaya, *Ketika Hukum Berhadapan Dengan Globalisasi*, UB Press, Malang, 2011, h. 4.

teknologi *e-banking* dan banyak hal lain yang terasa sangat mudah untuk dilakukan dibanding sebelumnya".[2]

Adapun "Jaringan *borderless* merupakan jaringan yang disediakan untuk memudahkan pengguna internet agar dapat mengakses informasi seluas-luasnya".[3] Perpaduan antara teknologi komputer dan teknologi telekomunikasi membentuk sebuah piranti baru dengan nama internet. "Pada intinya, internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optic, satelit atau gelombang frekuensi".[4]

Di dalam jaringan *borderless* bukan hanya ada individu atau perorangan yang menjadi subjek, negara juga termasuk. Sama halnya dengan individu, cara negara berhubungan dengan negara lain kini makin maju dengan internet dan jaringan telekomunikasi lain. Meskipun dalam hal ini kegiatan diwakili oleh orang, namun dilakukan atas nama negara. Menghubungi kepala negara lain, perdana menteri, atau menteri luar negeri hanya perlu menggunakan telepon. Mengirim surat menggunakan surat elektronik atau *e-mail*, lebih mudah dari sebelumnya yang harus mengirim surat menggunakan jasa pengiriman sehingga memakan waktu lama jika letak negara yang dituju jauh. Selain itu, juga bermafaat sebagai media publikasi mengenai konvensi-konvensi baru yang dibuat dan diratifikasi oleh negara-negara dalam hal perjanjian internasional serta peraturan-peraturan baru yang dibuat oleh pemerintah dalam satu negara.

---

[2] *Ibid.*

[3] Intan Innayatun Soeparna, *Kejahatan Telematika Sebagai Kejahatan Transnasional*, diakses melalui : http://www.academia.edu/208360/Kejahatan-Telematika-sebagai-Kejahatan-Transnasional, diakses pada tanggal 04 Desember 2024.

[4] Agus Raharjo, *Cybercrime*, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Citra Aditya Bakti, Bandung, 2002, h. 59.

Cyber crime, merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai alat kejahatan utama. "*Cyber crime* yang menggunakan media komunikasi dan komputer, kendati berada di dunia lain dalam bentuk maya tetapi memiliki dampak yang sangat nyata".[5] Penyimpangan dan kerugian telah terjadi dan dirasakan oleh masyarakat di seluruh penjuru dunia tidak terkecuali di Indonesia. Kerugian berdampak di sektor-sektor lain dibidang ekonomi, perbankan, moneter, dan sektor lain yang menggunakan jaringan komputer.

Perkembangan teknologi informasi di bidang *cyber* semakin membuka peluang bagi setiap negara yang berambisi untuk menaklukkan Indonesia maupun negara-egara lain dalam melakukan aksi spionase melalui penyadapan. Aksi ini yang dikenal dengan *cyber espionage* menjadi semakin marak dan semakin mudah dilakukan karena regulasi yang mengatur tentang perbuatan Spionase melalui penyadapan masih menampakkan kelemahannya dalam mencakup permasalahan ini. Mengingat *Spionase* atau aksi mata-mata yang dilakukan melalui cara-cara peperangan sangat jauh berbeda dengan dengan aksi mata-mata yang dilakukan tanpa adanya peperangan yaitu melalui penyadapan. Hal inilah yang justru menjadi kelemahan Pemerintah Indonesia dalam mengambil sikap dan menentukan arah kebijakan terhadap kasus *cyber espionage*.

Secara etimologis, kata "spionase" berasal dari bahasa Prancis "*espionage*" yang berarti pengintaian. "Menurut *Cambridge Dictionary*, spionase artinya

[5] Sutarman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, Laks Bang PRESSindo, Jogjakarta, 2007, h. 3.

menemukan informasi rahasia, khususnya informasi militer atau politik dari negara lain atau informasi industrial dari suatu bisnis".[6] Sedangkan menurut "*Nolo's Plain-English Law Dictionary*, spionase adalah tindakan memata-matai atau mengawasi aktivitas suatu pemerintahan atau perusahaan dengan tujuan untuk mengumpulkan informasi rahasia".[7]

Hukum internasional telah mengatur tentang spionase dalam masa perang. "Salah satu kodifikasi awal terkait spionase dalam masa perang di era modern dapat dilihat dalam Deklarasi Brussels 1874. Deklarasi ini tidak diadopsi oleh para pihak",[8] namun aturan-aturan di dalamnya berguna untuk memberikan definisi spionase dan kriteria mata-mata atau pelaku spionase. Aturan-aturan tentang spionase lainnya dapat dilihat dalam berbagai macam instrumen hukum internasional seperti Konvensi Den Haag 1899 dan 1907, *Hague Rules of Air Warfare* 1923, Konvensi Jenewa 1949 dan Protokol Tambahan 1977.

Deklarasi Brussels 1874, Konvensi Den Haag 1899 dan 1907, dan *Hague Rules of Air Warfare* 1923 memiliki kriteria yang sama untuk mata-mata atau pelaku spionase dengan pemilihan kata yang sedikit berbeda, namun tidak memengaruhi arti secara keseluruhan. Kriteria seorang mata-mata atau pelaku spionase menurut instrumen-instrumen tersebut antara lain: 1) Bertindak secara sembunyi-sembunyi atau di bawah alasan palsu, 2) Memperoleh atau berusaha

---

[6] Cambridge Dictionary, *Espionage (Online),* diakses melalui : https://dictionary.cambridge.org/dictionary/english/espionage, diakses pada tanggal 04 Desember 2024.

[7] Cornell Law School, *Espionage (Online),* diakses melalui : https://www.law.cornell.edu/wex/category/international_law?page=3, diakses pada tanggal 04 Desember 2024.

[8] International Committee of the Red Cross, *Project of an International Declaration Concerning the Laws and Customs of War, Brussels, 27 August 1874 (Online),* diakses melalui : https://ihl-databases.icrc.org/ihl/INTRO/135, diakses pada tanggal 04 Desember 2024.

untuk memperoleh informasi, 3) Dari wilayah lawan atau zona operasi belligerent, dan 4) Bermaksud untuk menyampaikan informasi yang telah didapat kepada pihak yang berlawanan.

Konvensi Jenewa ke-IV tahun 1949 dan Protokol Tambahan 1977 mengatur tentang perlakuan terhadap seseorang yang dianggap telah melakukan spionase. Pasal 5 Konvensi Jenewa 1949 ke-IV menyatakan bahwa saat seorang individu yang dilindungi ditahan sebagai pelaku spionase atau sabotase, maka orang tersebut akan dianggap telah kehilangan hak berkomunikasi di bawah aturan Konvensi. Namun, individu tersebut harus tetap diperlakukan secara manusiawi dan tetap memiliki haknya atas pengadilan yang adil, juga hak dan keistimewaan penuh yang diberikan pada orang yang dilindungi di bawah Konvensi. Pasal 46 ayat (1) Protokol Tambahan 1977 ke-I mengatur bahwa anggota pasukan bersenjata dari suatu Pihak dalam konflik atau sengketa yang jatuh ke dalam kekuasaan lawan ketika sedang melakukan tindakan spionase tidak akan mempunyai hak atas status tawanan perang, dan akan diperlakukan sebagai mata-mata.

"Kejahatan berbasis dunia maya atau kejahatan *cyber* telah menjadi ancamam nyata bagi negara di seluruh dunia. Peningkatan kasus kejahatan *cyber* terjadi dengan significant".[9] Salah satu bentuk dari kejahatan *cyber* adalah spionase siber atau mata-mata siber. spionase siber dapat menyebabkan terganggunya ekonomi, keamananan, dan juga hubungan antar negara. "Meskipun mempunyai dampak yang membahayakan negara, kasus spionase siber ini sulit

[9] Attacks in International Law, *PHD Thesis University of Glasgow Scotlandia*, diakses melalui : https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime, diakses pada tanggal 04 Desember 2024.

untuk diselesaikan karena identitas penyerang tidak mudah untuk diketahui secara pasti".[10]

Dapat dilihat bahwa aktivitas *cyber espionage* atau memasuki jaringan siber suatu negara secara tidak sah serta mengambil data dan informasi sesitif milik negara lain telah menimbulkan banyak kerugian bagi negara yang mengalaminya. Kerugian yang diterima dapat dalam bentuk ekonomi melihat beberap arsip rahasia seperti data kekayaan intelektual dan data mengenai peluang restrukturisasi perusahaan-perusahaan dalam negeri dapat diketahui oleh pihak lain, pada akhirnya berdampak pada kondisi perekonomian suatu negara. Dengan adanya praktik tersebut beberapa strategi dan langkah kebijakan suatu negara dapat diketahui oleh negara lain yang kemudian menimbulkan dampak yang sangat signifikan terhadap berjalannya suatu negara.

Sebagaimana contoh kasus di Indonesia mengenai salah satu perang siber yang paling menghebohkan di Indonesia adalah aksi para hacker Indonesia terhadap Australia. Kasus ini bermula ketika Edward Snowden, mantan perwira intelijen Amerika Serikat (AS), mengatakan bahwa Australia telah menguping Presiden Susilo Bambang Yudhoyono (SBY). Hal ini memicu kemarahan para hacker Indonesia karena lahirnya Anonymous Indonesia. Komunitas ini juga telah menciptakan gerakan *Stop Spying* Indonesia dengan menyerang website Australia dengan berbagai cara. Ambil contoh serangan *Distributed Denial of Service* (DdoS). Tentara siber Indonesia membanjiri server situs *web* Australia dengan permintaan palsu hingga kelebihan beban dan situs tersebut tidak dapat diakses

[10] Dana Rubenstein, *Nation State Spionase Cyber and its Impacts,* Paper Washington University, St. Louis, 2014, h. 7.

lagi. Salah satu korban adalah situs web Polisi Federal Australia. Masih berlanjut, Anonymous Indonesia juga melakukan perusakan ratusan website sipil secara acak. Serangan tersebut menyebabkan situs belanja kelas bawah di Australia menampilkan peringatan dari Indonesia. Tentara siber Australia tidak tinggal diam. Mereka membalas dengan menghapus banyak situs populer Indonesia. Seperti KPK (Komisi Pemberantasan Korupsi), PLN (Portal Layanan Pelanggan), Garuda Indonesia, Polri (Polisi Republik Indonesia), dan lain-lain.

Korban *cyber espionage* adalah pihak yang dirugikan akibat tindakan pengumpulan informasi secara *ilegal* melalui dunia maya. Korban *cyber espionage* adalah individu, organisasi, atau negara yang terkena dampak dari aktivitas pengumpulan informasi secara *ilegal* melalui teknologi informasi dan komunikasi. *Cyber espionage* umumnya menargetkan data rahasia atau sensitif, seperti informasi politik, militer, ekonomi, atau intelektual lainya.

Isu hukum dalam penelitian ini bahwa *cyber espionage* merupakan kejahatan hukum lintas Negara, Jika pelaku berada di luar yurisdiksi Indonesia, penegakan hukum menjadi lebih kompleks. Dan belum adanya pengaturan khusus tentang *cyber espionage*, sehingga terdapat kekosongan hukum karena tidak ada regulasi yang secara spesifik menyebutkan istilah *cyber espionage* sehingga penegak hukum mengandalkan pengaturan yang relevan secara umum saja.

Dengan berlandaskan latar belakang tersebut penulis tertarik untuk melakukan sebuah penelitian ilmiah dalam bentuk skripsi dengan judul Pertanggungjawaban Tindak Pidana *Cyber Espionage* Di Indonesia.

1.2. Rumusan Masalah

Dari rangkaian latar belakang masalah yang telah di uraikan di atas dapat di rumuskan masalah yang hendak dikaji adalah :

1. Bagaimana pengaturan tindak pidana *cyber espionage* dalam hukum positif di Indonesia ?
2. Bagaimana pertanggungjawaban pelaku tindak pidana *cyber espionage* berdasarkan hukum positif di Indonesia ?

1.3. Tujuan Penelitian

Adapun dalam penelitian ini merupakan sebuah kegiatan yang bertujuan sebagai berikut :

1. Untuk mengetahui dan memahami, pengaturan tindak pidana *cyber espionage* dalam hukum positif di Indonesia.
2. Untuk mengetahui dan memahami bentuk pertanggungjawaban pelaku tindak pidana *cyber espionage* berdasarkan hukum positif di Indonesia.

1.4. Manfaat Penelitian

Melalui penelitian ini diharapkan dapat memberikan manfaat dalam ilmu pengetahuan hukum, baik secara teoritis maupun secara prakti, yaitu:

1. Secara teoritis penelitian ini dapat memberikan kontribusi pemikiran dalam rangka pengembangan khasanah ilmu pengetahuan khususnya dibidang hukum pidana mengenai pengaturan hukum terkait tindak pidana *cyber espionage* di Indonesia berdasarkan hukum positif di Indonesia.
2. Secara praktis penelitian ini dapat menjadi salah satu landasan hukum, rujukan dan/atau referensi sesuai ketentuan hukum mengenai pengaturan

hukum terkait tindak pidana kejahatan *cyber espionage* berdasarkan hukum positif di Indonesia.

1.5. Tinjauan Pustaka

Dalam penelitian skripsi ini, peneliti menggali informasi dari pendapat para ahli hukum, teori-teori, asas-asas hukum dan beberapa peraturan yang menjadi konstruksi berfikir dalam menjawab pokok permasalahan.

1.5.1. Landasan Konseptual

Landasan konseptual merupakan suatu pengarah, atau pedoman yang lebih konkrit berisikan konsep-konsep umum atau tinjauan umum ketentuan dan pengertian serta hal hal yang berhubungan dengan pokok penelitian, adapun landasan konseptual dalam penelitian ini yaitu: a) *Cyber Crime* dan Karakteristiknya; b) Bentuk-Bentuk Kejahatan *Cyber*; c) Hukum Dunia Maya (*Cyber Law*)

a) *Cyber Crime* dan Karakteristiknya

Cyber crime pada awalnya diartikan sebagai kejahatan komputer (*computer crime*). *The British Law Commission* mengartikan *computer crime* sebagai manipulasi komputer yang dilakukan dengan itikad buruk agar bisa mendapatkan uang, barang, atau keuntungan yang lain atau dapat pula diartikan sebagai timbulnya kerugian bagi pihak lain. Mandell membagi *computer crime* atas 2 (dua) kegiatan, yaitu:[11]

1) Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembunyian untuk bisa mendapatkan keuangan, keuntungan, bisnis, kekayaan atau pelayanan; dan

[11] Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers, Jakarta, 2012, h. 10.

2) Ancaman bagi komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi itu sendiri serta sistem informasi yang sebagai sarana untuk menyampaikan atau melakukan pertukaran informasi kepada pihak lainnya. "*Computer crime* merupakan tindak kejahatan yang tidak melibatkan jaringan dan internet tetapi hubungan antara tindak kejahatan dengan komputer sebagai sarana kejahatannya, sedangkan *cyber crime* merupakan tindak kejahatan dengan menggunakan koneksi internet bahkan bisa menembus negara lain".[12]

Di bidang teknologi informasi kejahatan dapat digolongkan dalam *white colour crime* karena pelaku *cyber crime* adalah mereka yang mengerti dan menguasai penggunaan internet serta aplikasi yang ada atau biasa disebut sebagai orang yang ahli dalam bidangnya. *Cyber crime* memiliki beberapa karakteristik yaitu:[13]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah, siber/*cyber*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya;
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet;
c. Perbuatan tersebut mengakibatkan kerugian berupa materil dan inmateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya; dan
e. Perbuatan tersebut saring dilakukan secara transnasional atau melintas batas negara.

---

[12] Maskun dan Wiwik Meilarati, *Aspek Hukum Penipuan Berbasis Internet*, Keni Media, Bandung, 2017, h. 20.

[13] Budi Sahariyanto, *Op.Cit.*, h. 11.

b) Bentuk-Bentuk Kejahatan *Cyber*

Ari Juliano Gema menyatakan bahwa kejahatan siber dapat dikelompokkan menjadi beberapa bentuk, yaitu:[14]

1. *Unauthorized Acces to Computer System and Service*;
   Kejahatan ini dilakukan dengan cara memasuki/ menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau dengan melawan hukum. Contoh bentuk kejahatan siber ini yaitu *cracking*, *hacking*.
2. *Iilegal Content*;
   Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh bentuk kejahatan ini yaitu conten porno grafi, berita bohong/*hoax*.
3. Data *Forgery*;
   Merupakan kejahatan dengan memalsukan data pada dokumen dokumen penting yang tersimpan sebagai *scriptless documen* melalui internet.
4. *Cyber Espionage*;
   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata dengan memasuki sistem jaringan komputer pihak sasaran.
5. *Cyber Sabotage and Extortion*;
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Contoh bentuk kejahatan ini yaitu penanaman *malware*/ virus.
6. *Offence Againts Intellectual Property*; dan
   Kejahatan ini berupa pelanggaran HKI yang dimilki pihak lain di Internet. Contoh bentuk kejahatn ini misalnya *cloning, phising web*.
7. *Infringement of Privacy.*
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Informasi yang dimaksud seperti Pin ATM, Nomor Kartu Kredit, NIK dan sebagainya. Contoh bentuk kejahatan ini yaitu pencurian data pribadi.

c) Hukum Dunia Maya (*Cyber Law*)

[14] Wahid, Abdul dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005, h. 72.

Cyber law ini bertumpu pada disiplin ilmu hukum yang terdahulu antara lain: HAKI (Hak Atas Kekayaan Intelektual), hukum perdata, hukum perdata internasional dan hukum internasional. "Hal ini mengingat ruang lingkup *cyber law* yang cukup luas. Karena saat ini perkembangan transaksi on line (*e-commerce*) dan program *egovernment* pada 9 Juni 2003 pasca *USA E-Government Act* 2002 *Public Law* semakin pesat".[15]

Menurut Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar dalam Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi menyatakan bahwa meskipun belum ada kesamaan dan kesepahaman mengenai definisi dari *Cyber Crime*, namun ada beberapa kesamaan pengertian mengenai kejahatan siber ini, yaitu dengan kehadiran komputer yang sudah mengglobal mendorong terjadinya aksi kejahatan siber ini. "Secara sederhana, aksi kejahatan siber (*Cyber Crime*) dapat diartikan sebagai jenis kejahatan yang dilakukan dengan menggunakan media Internet sebagai alat bantunya".[16]

Yurisdiksi adalah suatu kewenangan yang dimiliki oleh suatu negara untuk melaksanakan hukum nasional yang berlaku di negaranya terhadap orang, benda, dan peristiwa hukum di wilayah negaranya. Menurut Csabafi 1971 mengatakan bahwa Yurisdiksi Negara dalam hukum internasional berarti Hak dari suatu Negara untuk mengatur dan mempengaruhi dengan

---

[15] Ridhokudik, *Artikel Tentang Cyber Law*, diakses melalui : http://ridhosukamusik. blogspot.co.id/ 2010/10/artikel-tentang-cyber-law.html, diakses pada tanggal 04 Desember 2024.

[16] Mas Wigrantoro Roes Setiyadi dan Mirna Dian Avanti Siregar, *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, Global Internet PolicyInitiative-Indonesia Bekerja Sama Dengan Indonesia Media Law and Policy Center, November, 2003.

langkah-langkah dan tindakan yang bersifat legislatif, eksekutif, dan yudikatif atas hak-hak individu, milik atau harta kekayaannya, perilaku-perilaku atau peristiwa peristiwa yang tidak semata-mata merupakan masalah dalam negeri.

Dengan ruang lingkup yang cukup luas dan tanpa batas perlu sebuah produk hukum yang mennyangkut semua aspek *cyber law*. Dalam hukum internasional ada 3 (tiga) jenis yuridiksi yaitu:[17]

1) Yurisdiksi untuk menetapkan Undang-Undang (*the jurisdiction to prescribe*);
2) Yurisdiksi untuk penegakan hukum (*the jurisdiction to enforce*); dan
3) Yuridiksi untuk menuntut (*the jurisdiction to adjudicate*).

Cyber crime merupakan suatu kejahatan mayantara yang dapat dilakukan tanpa mengenal batas ruang dan waktu, diperlukan suatu upaya pencegahan untuk menanggulangi kejahatan tersebut. Aktivitas pokok dari *cyber crime* adalah penyerangan terhadap *computer system* dan *communication system* milik orang lain atau umum di dalam *cyber space*. Fenomena *cyber crime* memang harus diwaspadai karena kejahatan ini berbeda dengan kejahatan lain pada umumnya. *Cyber space, cyber crimes,* dan *cyber laws* merupakan bagian yang tidak dapat terpisahkan dari teknologi informasi dan komunikasi saat ini.

Terminologi-terminologi ini semakin populer dibahas di berbagai media cetak maupun elektronik, oleh pengamat dalam surat kabar,

[17] Warta Warga Gunadarma, *Cyber Crime di Dunia Maya*, diakses melalui: http://wartawarga.gunadarma.ac.id/2010/03/cyber-chrime-di-dunia-maya, diakses pada tanggal 04 Desember 2024.

akademisi dalam berbagai jurnal ilmiah, dan juga termasuk oleh pemerintah dalam pembentukan peraturan perundang-undangan ataupun hukum yang mengatur seluruh kegiatan di dunia *cyber* tersebut. "Aspek hukum dalam rezim hukum 3 (tiga) *cyber* cukup luas, yaitu dalam hukum administrasi, perdata, dan pidana. Ketiga bidang hukum *cyber* tersebut dapat disebut *sebagai cyber law*".[18]

1.5.2. Landasan Yuridis

Landasan yuridis merupakan dasar hukum yang mengatur dan berhubungan dengan objek penelitian. Landasan yuridis dalam penelitian ini berkaitan dengan tindak pidana *cyber espionage*. Landasan yuridis terkait *cyber espionage* (spionase siber) berakar pada hukum internasional, nasional, dan kebijakan yang berlaku di berbagai negara. *Cyber espionage* melibatkan tindakan pengumpulan informasi rahasia secara ilegal melalui teknologi informasi dan komunikasi. Berikut adalah beberapa landasan yuridis diantaranya:

1) Hukum Internasional
    a. *Budapest Convention on Cybercrime* (2001): Konvensi ini bertujuan untuk mengatasi kejahatan dunia maya termasuk akses *ilegal*, pelanggaran data, dan intersepsi yang tidak sah. Meskipun tidak secara eksplisit menyebutkan spionase siber, ketentuannya mencakup aktivitas yang sering digunakan dalam spionase siber.

[18] Widodo, *Hukum Pidana di Bidang Teknologi Informasi, Cyber Crime Law: Telaah Teoritik dan Bedah Kasus,* Aswaja Pressindo, Yogyakarta, 2013, h. 5.

b. *United Nations Charter* (1945): Pasal 2 ayat (4) melarang penggunaan kekuatan terhadap kedaulatan negara lain, yang dapat mencakup aktivitas siber yang mengancam keamanan nasional suatu negara.

c. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013): Manual ini memberikan panduan tentang bagaimana hukum internasional berlaku dalam konflik siber, termasuk tindakan spionase siber yang dapat dianggap sebagai pelanggaran hukum perang.

2) Hukum Nasional (Indonesia)

a. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE): Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik mengatur tentang larangan akses ilegal ke sistem elektronik milik orang lain, yang dapat mencakup aktivitas spionase siber. Dan Pasal 31 Undang-Undang Informasi dan Transaksi Elektronik melarang intersepsi atau penyadapan ilegal terhadap informasi elektronik.

b. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: Undang-Undang ini menjadi dasar hukum utama untuk penindakan kejahatan siber di Indonesia, termasuk aktivitas yang berkaitan dengan pengumpulan informasi rahasia secara ilegal.

c. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme: Jika spionase siber berkaitan dengan aksi terorisme, maka dapat dikenakan sanksi berdasarkan Undang-Undang ini.

d. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara: Undang-Undang ini memberikan kewenangan kepada lembaga intelijen untuk melakukan operasi pengumpulan informasi, namun juga mengatur batasan untuk mencegah penyalahgunaan.

Banyak negara belum memiliki aturan khusus terkait spionase siber. Hal ini menyulitkan penegakan hukum di wilayah abu-abu antar negara. Serta tidak semua bentuk *cyber espionage* dianggap melanggar hukum. Misalnya, pengumpulan informasi melalui metode yang tidak langsung melanggar hukum sering kali berada di area abu-abu hukum. Regulasi terkait spionase siber terus berkembang seiring dengan meningkatnya ancaman dunia maya. Diperlukan koordinasi antara hukum nasional dan internasional untuk menangani tantangan yang muncul akibat tindakan ini.

1.5.3. Landasan Teori

Landasan teori merupakan teori-teori yang digunakan oleh penulis sebagai dasar atau pedoman berpikir dalam penelitian. Adapun landasan teori dalam penelitian ini merupakan teori perlindungan hukum.

> Menurut Fitzgerald sebagaimana dikutip Satjipto Raharjo awal mula dari munculnya teori perlindungan hukum ini bersumber dari teori hukum alam atau aliran hukum alam. Aliran ini dipelopori oleh Plato, Aristoteles (murid Plato), dan Zeno (pendiri aliran Stoic). Menurut aliran hukum alam menyebutkan bahwa hukum itu bersumber dari Tuhan yang bersifat universal dan abadi, serta antara hukum dan

> moral tidak boleh dipisahkan. Para penganut aliran ini memandang bahwa hukum dan moral adalah cerminan dan aturan secara internal dan eksternal dari kehidupan manusia yang diwujudkan melalui hukum dan moral.[19]
>
> Fitzgerald menjelaskan teori pelindungan hukum Salmond bahwa hukum bertujuan mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat karena dalam suatu lalu lintas kepentingan, perlindungan terhadap kepentingan tertentu hanya dapat dilakukan dengan cara membatasi berbagai kepentingan di lain pihak. Kepentingan hukum adalah mengurusi hak dan kepentingan manusia, sehingga hukum memiliki otoritas tertinggi untuk menentukan kepentingan manusia yang perlu diatur dan dilindungi. Perlindungan hukum harus melihat tahapan yakni perlindungan hukum lahir dari suatu ketentuan hukum dan segala peraturan hukum yang diberikan oleh masyarakat yang pada dasarnya merupakan kesepakatan masyarakat tersebut untuk mengatur hubungan prilaku antara anggota-anggota masyarakat dan antara perseorangan dengan pemerintah yang dianggap mewakili kepentingan masyarakat.[20]

Dalam Kamus Besar Bahasa Indonesia (KBBI). Perlindungan berasal dari kata lindung yang memiliki arti mengayomi, mencegah, mempertahankan, dan membentengi. Sedangkan Perlindungan berarti konservasi, pemeliharaan, penjagaan, asilun, dan bunker. Secara umum, perlindungan berarti mengayomi sesuatu dari hal-hal yang berbahaya, sesuatu itu bisa saja berupa kepentingan maupun benda atau barang. Selain itu perlindungan juga mengandung makna pengayoman yang diberikan oleh seseorang terhadap orang yang lebih lemah. Dengan demikian, perlindungan hukum dapat diartikan Perlidungan oleh hukum atau perlindungan dengan menggunakan pranata dan sarana hukum.

---

[19] Satjipto Raharjo,*Ilmu Hukum*, PT Citra Aditya Bakti, Bandung, 2000, h. 53.
[20] Ibid, h. 54.

Adapun pendapat yang dikutip dari beberapa ahli mengenai perlindungan hukum sebagai berikut, yaitu:[21]

1. Menurut Satjito Rahardjo perlindungan hukum adalah adanya upaya melindungi kepentingan seseorang dengan cara mengalokasikan suatu Hak Asasi Manusia kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut;
2. Menurut Setiono perlindungan hukum adalah tindakan atau upaya untuk Melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum, untuk mewujudkan ketertiban dan ketentraman sehingga memungkinkan manusia untuk menikmat martabatnya sebagai manusia;
3. Menurut Muchsin perlindungan hukum adalah kegiatan untuk melindungi individu dengan menyerasikan hubungan nilai-nilai atau kaidah-kaidah yang menjelma dalam sikap dan tindakan dalam menciptakan adanya ketertiban dalam pergaulan hidup antara sesama manusia; dan
4. Menurut Philipus M. Hadjon Selalu berkaitan dengan kekuasaan. Ada dua kekuasaan pemerintah dan kekuasaan ekonomi. Dalam hubungan dengan kekuasaan pemerintah, permasalahan perlindungan hukum bagi rakyat (yang diperintah), terhadap pemerintah (yang memerintah). Dalam hubungan dengan kekuasaan ekonomi, permasalahan perlindungan hukum adalah perlindungan bagi si lemah (ekonomi) terhadap si kuat (ekonomi), misalnya perlindungan bagi pekerja terhadap pengusaha.

Pada dasarnya perlindungan hukum tidak membedakan terhadap kaum pria maupun wanita. Indonesia sebagai negara hukum berdasarkan pancasila haruslah memberikan perlindungan hukum terhadap warga masyarakatnya karena itu perlindungan hukum tersebut akan melahirkan pengakuan dan perlindungan hak asasi manusia dalam wujudnya sebagai makhluk individu dan makhluk sosial dalam wadah negara kesatuan yang menjunjung tinggi semangat kekeluargaan demi mencapai kesejahteraan bersama.

[21]Asri Wijayanti, *Strategi Penulisan Hukum*, Lubuk Agung, Bandung, 2011, h. 10.

1.6. Penelitian Terdahulu

Dalam penelitian yang dilakukan penulis, terdapat beberapa penelitian yang terdahulu sebagai bahan rujukan dan masukan dalam penelitian ini yaitu:

1. Rofi'a Zulkarnain. Skripsi dengan judul Tindakan Spionase Melalui Penyadapan Antar Negara Sebagai *Cybercrime*, Fakultas Hukum Universitas Brawijaya Malang 2014. Hasil penelitian menunjukkan bahwa Berdasarkan hukum nasional Indonesia, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tindakan yang dilakukan Australia melanggar hukum nasional Indonesia. Namun, dalam permasalahan ini tidak dapat begitu saja menerapkan hukum nasional meskipun tindakan yang dilakukan Australia adalah melanggar hukum nasional. Selain dengan penyelesaian melalui penyelesaian diplomatik. Persoalan antar negara ini juga dapat diselesaikan melalui Mahkamah Internasional atau *International Court of Justice*.[22]
2. Nabiila Azzahra Abdullah. Skripsi dengan judul Urgensi Pengaturan *Cyber Espionage* Dalam Masa Damai Ditinjau Dari Hukum Internasional. Fakultas Hukum Universitas Brawijaya Malang 2022. Hasil penelitian menunjukkan bahwa urgensi dibentuknya pengaturan terhadap *cyber espionage* muncul karena dilanggarnya prinsip kedaulatan wilayah, banyaknya kasus yang terjadi, dan adanya kekosongan hukum. Adanya pengaturan dapat menciptakan ketertiban antar negara dalam komunitas internasional. Di dalam peraturan *cyber espionage* dalam masa damai harus memenuhi aspek-aspek penting seperti definisi dan kriteria, klasifikasi metode *cyber espionage*, pembahasan tentang tindakan unlawful, dan prinsip *due diligence.* Untuk *economic cyber espionage*, beberapa ahli mengusulkan *World Trade Organization* (WTO) sebagai badan yang memberikan prosedur pengadilan, beserta perjanjian *Trade-Related Aspects of Intellectual Property Rights* (TRIPS) maupun Konvensi Paris sebagai dasar hukum.[23]
3. Shelly Nicco. Skripsi dengan judul Tindak Pidana *Cyber Espionage*. Fakultas Hukum Universitas Airlangga Surabaya 2010. Hasil penelitian menunjukkan bahwa Jenis *cyber crime* yang dirasa membahayakan khalayak dalam aktivitasnya adalah *cyber espionage* yang lazimnya disebut tindakan mata-mata atau pengintaian terhadap suatu data pihak lain, karna kejahatan jenis ini tergolong tindak kejahatan "abu-abu". Mengingat internet merupakan media lintas informasi yang berdampak luas, maka akses data yang menyangkut pihak lain patut menjadi perhatian dan dapat menjadi

---

[22] Rofi'a Zulkarnain, *Tindakan Spionase Melalui Penyadapan Antar Negara Sebagai Cybercrime*, Skripsi, Fakultas Hukum Universitas Brawijaya, Malang, 2014.

[23] Nabiila Azzahra Abdullah, *Urgensi Pengaturan Cyber Espionage Dalam Masa Damai Ditinjau Dari Hukum Internasional,* Skripsi, Fakultas Hukum Universitas Brawijaya, Malang, 2022.

kejahatan yang serius. Aksi pengintaian ini dilakukan dengan motif yang beragam. Diantaranya politik, ekonomi, ilmu pengetahuan, perdagangan.[24]

Perbedaan antara penelitian ini dengan penelitian terdahulu, yakni dalam penelitian ini lebih pada pengulasan materi tentang tindak pidana *cyber espionage*, dengan sebatas memberikan ulasan kasus pada latar belakang penelitian namun tidak menggunakan tekhnik studi kasus dalam penelitian ini. Oleh karena itu penelitian ini lebih memfokuskan pada materi tentang pertanggungjawaban tindak pidana *cyber espionage* di Indonesia.

Adapun yang menjadi persamaan antara penelitian ini dengan penelitian terdahulu yakni sama-sama meneliti tentang *cyber crime* serta kejahatan terkait *cyber espionage*.

1.7. Metode Penelitian

Metode penelitian ini merupakan cara yang digunakan untuk mendapatkan data serta memperoleh jawaban yang akurat atas rumusan masalah diatas dengan mencari dan mengelola data dalam suatu penelitian.

1.7.1. Jenis Penelitian

Jenis penelitian ini adalah penelitian hukum normatif, penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum. “Penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas

[24] Shelly Nicco, Tindak Pidana *Cyber Espionage*, Skripsi, Fakultas Hukum Universitas Airlangga, Surabaya, 2010.

hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti".[25]

Hasil dari penelitian ini memberikan diskripsi mengenai rumusan masalah yang diajukan, penelitian normatif hanya meneliti norma hukum, tanpa melihat praktek hukum di lapangan (*law in action*) mengenai penelitian terkait pertanggungjawaban tindak pidana *cyber espionage* di indonesia.

1.7.2. Metode Pendekatan

Metode pendekatan merupakan salah satu tahapan penelitian yang dimaksudkan untuk mengumpulkan bahan-bahan hukum dalam berbagai aspek untuk mencari jawaban atas permasalahan yang telah dirumuskan dalam penelitian ini. Adapaun dalam penelitian ini penulis menggunakan tiga metode pendekatan antara lain pendekatan konseptual (*conceptual approach*), pendekatan perundang-undangan (*statute approach*), dan pendekatan historis (*historical approach*).

a. Pendekatan Konseptual (*Conceptual Approach*).

   Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum. Dengan mempelajari pandangan-pandangan dan doktrin-doktrin di dalam ilmu hukum, peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum. Pendekatan konseptual dilakukan guna dijadikan sebagai acuan untuk membangun argumentasi hukum yang berkaitan

[25] Suyanto, *Penelitian Hukum Pengantar Penelitian Normatif Empiris dan Gabungan*, Cetakan Pertama, Unigres Press, Gresik, 2022, h. 88.

dengan pokok permasalahan dalam penelitian ini yakni mengenai pertanggungjawaban tindak pidana *cyber espionage* di indonesia.

b. Pendekatan Perundang-Undangan (*Statute Approach*).

Pendekatan perundang-undangan dilakukan dengan menelaah semua Undang-Undang dan regulasi yang bersangkut paut dengan isu karena yang akan diteliti adalah berbagai aturan hukum yang menjadi fokus sekaligus tema sentral suatu penelitian. Dilakukan dengan cara menelaah dan mengkaji semua peraturan perundang-undangan yang berkaitan dengan pokok permasalahan yang dirumuskan dalam penelitian ini. Pendekatan perundang-undangan ini digunakan untuk mendapatkan ketentuan-ketentuan hukum guna untuk mempelajari konsistensi dan kesesuaian antara Undang-Undang yang satu dengan Undang-Undang lainnya. Adapun pendekatan perundang-undangan dalam penelitian ini yakni Undang Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; dan Kitab Undang-Undang Hukum Pidana (KUHP).

c. Pendekatan Historis (*Historical Approach*).

Pendekatan historis dalam penelitian hukum adalah metode yang digunakan untuk memahami hukum dengan menelusuri asal-usul, perkembangan, dan evolusi suatu norma hukum atau sistem hukum dari masa ke masa. Pendekatan ini melihat konteks sejarah dari

pembentukan dan penerapan suatu aturan hukum untuk mengetahui mengapa dan bagaimana hukum tersebut muncul, berubah, atau tetap berlaku. Tujuan pendekatan historis untuk menjelaskan latar belakang sosial, politik, ekonomi, atau budaya dari suatu aturan hukum, menemukan akar pemikiran atau ide dasar yang mempengaruhi lahirnya suatu hukum, dan membandingkan hukum dari waktu ke waktu untuk melihat kontinuitas atau perubahan.

1.7.3. Sumber Bahan Hukum (*Legal Sources*)

Bahan hukum yang dikumpulkan dalam penulisan untuk menjawab isu hukum penulisan ini yaitu: bahan hukum primer; bahan hukum sekunder; dan bahan hukum tersier.

1. Bahan Hukum Primer

   Bahan Hukum Primer adalah bahan-bahan hukum yang mengikat seperti Norma dan Kaidah Dasar, Peraturan Dasar, Peraturan Perundang-Undangan. Bahan hukum primer yang digunakan adalah :

   a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
   b) Kitab Undang-Undang Hukum Pidana (KUHP);
   c) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
   d) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
   e) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara;
   f) Undang-Undang Nomor 13 Tahun 2016 tentang Perlindungan Saksi dan Korban;

g) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

h) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana; dan

i) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

2. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai bahan hukum primer seperti : buku-buku hukum, hasil-hasil penelitian, pendapat pakar hukum. Dalam penelitian ini penulis menggunakan buku, makalah, hasil penelitian dalam bidang hukum, internet yang berkaitan dengan penelitian yang penulis lakukan.

3. Bahan Hukum Tersier

Bahan-bahan yang memberikan informasi tentang bahan hukum primer dan bahan hukum sekunder seperti : Ensiklopedia hukum, kamus bahasa Indonesia, kamus hukum, internet, hal ini dilakukan untuk mendukung dan menunjang penelitian penulis.

1.7.4. Teknik Pengumpulan dan Pengolahan Bahan Hukum

Berisi uraian logis prosedur pengumpulan bahan-bahan hukum primer, skunder, serta bahan hukum tersebut diinventarisasi dan diklarifikasi

dengan menyesuaikan masalah yang dibahas. Dalam penelitian hukum normatif, teknik pengumpulan bahan hukum sebagai berikut:

Bahan hukum primer berupa perundang-undangan dikumpulkan dengan metode inventarisasi dan kategorisasi. Bahan hukum sekunder dikumpulkan dengan sistem kartu catatan (*card system*), baik dengan kartu ikhtiar (memuat ringkasan tulisan sesuai aslinya, secara garis besar dan pokok gagasan yang memuat pendapat asli penulis), maupun kartu ulasan (berupa analisis dan catatan khusus penulis).

Dalam penelitian hukum normatif yuridis, teknik pengumpulan bahan hukum sebagai berikut:

1) Bahan hukum priemer merupakan bahan hukum yang bersifat autoritatif artinya mempunyai otoritas. Bahan-bahan hukum primer terdiri dari perundang-undangan;
2) Bahan hukum sekunder berupa publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi. Publikasi tentang hukum meliputi buku-buku teks, kamus-kamus hukum, jurnal-jurnal hukum, dan media daring.

1.7.5. Teknik Analisa Bahan Hukum

Analisis bahan hukum dalam penelitian ini berdasarkan data yang ada dilakukan secara yuridis kualitatif, yaitu tidak hanya mengungkapkan kebenaran belaka tetapi juga memahami kebenaran tersebut menurut aturan perundang-undangan. Dengan memberikan gambaran permasalahan tentang pertanggungjawaban tindak pidana *cyber espionage* di Indonesia dianalisis

berdasarkan aturan hukum yang berlaku di Indonesia dan fakta di lapangan untuk kemudian diperoleh kesimpulan sebagai jawaban atas permasalahan yang diajukan.

1.8. Sistematika Penulisan

Untuk lebih mengetahui dan mempermudah dalam melakukan pembahasan, penganalisaan, dan penjabaran isi dari penelitian ini, maka dalam penulisan skripsi ini penulis menyusun sistematika penulisan sebagai berikut :

Bab I menerangkan Pendahuluan yang berisikan tentang latar belakang permasalahan, rumusan masalah, kajian pustaka, tujuan penelitian, manfaat penelitian, orisinalitas penelitian, kajian pustaka yang terdiri dari landasan teori dan penjelasan konsep, metode penelitian terdiri atas jenis penelitian, pendekatan masalah, sumber bahan hukum, teknik pengumpulan dan pengolahan bahan hukum, analisis bahan hukum, dan diakhiri dengan pertanggung jawaban sistematika.

Bab II membahas tentang Pengaturan Tindak Pidana *Cyber Espionage* Dalam Hukum Positif di Indonesia. Dengan Sub Bab diantaranya : Sejarah *Cyber Espionage*; Modus Operandi *Cyber Espionage*: Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Kitab Undang-Undang Hukum Pidana; Pengaturan Tindak Pidana *Cyber Espionage* Berdasrkan Undang-Undang Informasi Dan Transaksi Elektronik; Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Undang-Undang Telekomunikasi; Dan Pengaturan Kejahatan *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia

Bab III membahas tentang Pertanggungjawaban Pelaku Tindak Pidana *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia. Dengan Sub Bab diantaranya: Pertanggungjawaban Hukum; Pertanggungjawaban Pelaku *Cyber Espionage* Berdasarkan Kitab Undang-Undang Hukum Pidana; Pertanggungjawaban Pelaku *Cyber Espionage* Diluar Kitab Undang-Undang Hukum Pidana; Pertanggungjawaban Pelaku *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia.

Bab IV sebagai penutup, memuat beberapa kesimpulan dari jawaban permasalahan-permasalahan yang dibahas, serta sebagai saran bagi pihak yang berkaitan dalam penulisan skripsi ini.