BAB LENGKAP-6.doc

by . .

Submission date: 23-Jul-2025 04:07PM (UTC+0700)
Submission ID: 2719404988
File name: BAB_LENGKAP-6.doc (305K)
Word count: 16061
Character count: 107054

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.

BAB II

PENGATURAN TINDAK PIDANA *CYBER ESPIONAGE* BERDASARKAN HUKUM POSITIF DI INDONESIA

2.1. Sejarah *Cyber Espionage*

"Spionase berasal dari bahasa Perancis yakni *espionnage* yang merupakan suatu praktik untuk mengumpulkan informasi mengenai sebuah organisasi atau lembaga yang dianggap rahasia tanpa mendapatkan izin yang sah dari pemilik informasi tersebut".[26] Sejarah mengenai spionase ini sendiri pun terdokumentasi dengan baik dimulai dari sejak jaman-jaman kekaisaran hingga jaman modern sekarang ini di berbagai belahan dunia. Salah satu cerita mengenai spionase berawal dari kisah Chandragupta Maurya seorang pendiri kekaisaran Maurya di India yang memanfatkan pembunuhan, mata-mata sebagai bagian dari upaya spionase dan agen rahasia yang dijelaskan secara gamblang pada Chanakya Arthasastra.

Beranjak dari kisah tersebut, pada saat perang dingin berlangsung, kegiatan spionase telah dilakukan oleh Amerika Serikat, Uni Soviet, dan *People's Republic of China* dan sekutu mereka khususnya yang berkaiatan dengan aktivitas kepemilikan senjata nuklir rahasia. "Tidak seperti bentuk lain dari pengumpulan data intelejen, spionase biasanya melibatkan pengaksesan tempat penyimpanan informasi yang diinginkan, atau mengakses orang-orang yang mengetahui

[26] Wikipedia, *Spionase*, diakses melalui: www.Wikipedia/spionase.com, diakses pada tanggal 1 Mei 2025.

mengenai informasi tersebut dan akan membocorkannya melalui berbagai dalih".[27]

> *The US* mendefinisikan spionase sebagai "Tindakan memperoleh, memberikan, mengirimkan, berkomunikasi, atau menerima informasi mengenai pertahanan nasional dengan tujuan atau alasan untuk percaya, bahwa informasi dapat digunakan untuk mencederai Amerika atau bangsa asing. Sedangkan *Black's Law Dictionary* (1990) mendefinisikan spionase *"The practice of using spies to collect information abaout what another government or company is doing or plans to do*.[28]

Salah Satu kasus mengenai spionase yang sangat fenomenal terjadi ketika Perang Dunia I. Saat itu seorang wanita Belanda bernama Margareth Getruide Zelle yang lebih terkenal dengan nama Mata Hari merupakan penari orientalis dan spion politik untuk pemerintah Jerman. Ketika berusia 19 tahun dia dinikahi oleh Rudolp McLeod yang merupakan Perwira Tinggi Militer Belanda yang bertugas di Indonesia sehingga kemudian tinggal berpindah-pindah di berbagai kota di Indonesia, salah satunya adalah kota Malang dan Semarang.

Sebelum terjun di dunia spionase, wanita yang memilki kode rahasia H21 ini mengawali karirnya sebagai penari erotis di Paris. Berbekal keahlian *erotic temple dance* yang dipelajari di India serta tarian-tarian daerah selama tinggal di Indonesia dan daya pikatnya yang tinggi, dia menjadi terkenal dimana-mana. Tak heran bila kemudian tawaran menari banyak berdatangan dari kota-kota besar di Eropa bahkan Mesir. Kondisi inilah yang kemudian menyeretnya dalam dunia spionase. Saat menjadi *stripper* di Berlin, agen rahasia Jerman merekrutnya. Mata hari kemudian sering berkelana baik antar kota maupun antar negeri. Karena

---

[27] *Ibid*.

[28] Shelly Nicco, *Tindak Pidana Cyber Espionage*, Skripsi, Fakultas Hukum Universitas Airlangga, Surabaya, 2010, h. 20.

sering bepergian, maka dia tidak punya kesulitan untuk menyusup, termasuk dalam masa Perang Dunia Pertama.

Agen rahasia Inggris yang mempunyai kode M15 mulai curiga dengan aktivitas yang dilakukan oleh Mata Hari. Agen rahasia Inggris tersebut lalu mengintrogasinya, namun mereka tidak bisa memaksa Mata Hari untuk membuka mulut. Bekali-kali interogasi dilakukan namun hasilnya tetap nihil. Sampai akhirnya Agen rahasia Perancis berhasil menangkap dan mengintrogasinya saat dia menyebrangi Perancis untuk mengunjungi salah satu *affair*nya. "Agen rahasia Perancis menangkap Mata Hari karena diyakini dialah "*The Greatest Woman Spy*" yang harus bertanggung jawab atas kematian beribu-ribu tentara akibat informasi yang diberikannya. Dia lalu diadili di pengadilan perang dan dieksekusi dihadapan regu tembak pada tanggal 15 September 1917".[29]

"Perkembangan spionase, yang awalnya hanya digunakan atau dianggap sebagai upaya institusional dengan cara memata-matai musuh potensial atau aktual, terutama untuk tujuan militer, kini telah berkembang untuk memata-matai perusahaan, yang kini dikenal secara spesifik sebagai Spionase Industrial".[30] Dalam perjalanan spionase industrial ini, satu kasus besar yang pernah terjadi adalah kasus spionase yang melibatkan dua perusahaan otomotif dunia terbesar peserta Formula 1 yakni McLarren Mercedes dengan Ferrari.

---

[29] Wikipedia, *Matahari*, diakases melalui: http://wikipeda.org/wiki/Mata_Hari.com, diakses pada tanggal 1 Mei 2025.

[30] Wikipedia, *Sejarah Espionase*, diakses melalui: www.wikipedia/spionase/sejarah.com, diakses pada tangal 1 Mei 2025.

2.2. Modus Operandi *Cyber Espionage*

Modus operandi merupakan cara-cara yang digunakan sebagai sarana untuk melakukan *cyber espionage*. *Cyber Espionage* lazimnya disebut tindakan mata-mata atau pengintaian terhadap suatu data pihak lain. Mengingat internet merupakan media lintas informasi yang berdampak luas, maka akses data yang menyangkut pihak lain patut menjadi perhatian dan dapat menjadi kejahatan yang serius. Aksi pengintaian ini dilakukan dengan motif yang beragam. Diantaranya politik, ekonomi, ilmu pengetahuan, perdagangan, dan lain sebagainya.

Dalam sistem hukum dan kehidupan sehari-hari, keberadaan suatu arsip berupa data dan/atau informasi elektronik adalah dimaksudkan sebagai suatu alat bukti yang merekam/menerangkan keberadaan suatu informasi tertentu, atau dalam bahasa hukum ini dinyatakan sebagai pembuktian terhadap telah terjadinya suatu peristiwa hukum yang tentunya mempunyai akibat hukum tertentu bagi hak dan kewajiban para pihak yang tersangkut daripadanya. "Demikian juga adanya dengan arsip elektronik".[31] "Ada tiga macam data dan/atau informasi elektronik yang terdapat di internet yang dapat diakses secara bebas. Pertama adalah yang tersedia dalam bentuk basis data (*database*) *online*; kedua yang diperoleh dalam suatu transaksi *online;* dan ketiga yaitu basis data yang dimiliki oleh negara atau pemerintah yang terdapat dalam situs-situs pemerintah tersebut".[32]

Sedangkan Data dan/atau informasi yang umumnya dijadikan target atau sasaran dalam tindak pidana *cyber espionage* ini umumnya bukan merupakan

---

[31] Edmon Makarim, *Kompilasi Hukum Telematika,* PT Raja Grafindo Persada, Jakarta, 2004, h. 207.

[32] Susan E.Gindin, *Lost and Found in Cyberspace: Informational Privacy in The Age of The Internet*, Jurnal San Diego Law Review 1153, 1997.

informasi elektronik sembarangan maupun yang dapat diakses secara bebas, hal tersebut dapat dilihat dari nilai kualitas informasi itu sendiri yang tergantung pada 3 (tiga) hal yaitu informasi tersebut haruslah akurasi, ketepatan waktu, dan relevansi. Akurasi berarti informasi tersebut harus bebas dari kesalahan dan tidak bias. Akurat juga berarti bahwa informasi tersebut harus jelas maksud dan tujuan. "Ketepatan waktu berarti informasi tersebut bukan sesuatu yang sudah usang. Relevansi berarti informasi tersebut memiliki manfaat bagi pemakai atau pihak lain yang membutuhkan".[33]

Cara-cara yang dilakukan dalam proses pengintaian ini terjadi bila terjadi suatu akses ke dalam suatu sistem yang dituju mencapai suatu keberhasilan. Proses penyusupan hingga terjadi pengintaian secara sistematis melalui tahapan sebagai berikut :

1) *Footprinting* (Pencarian Data)

   Hacker baru mencari-cari sistem yang dapat disusupi. *Footprinting* merupakan kegiatan pencarian data berupa:

   a. Menentukan ruang lingkup (*scope*) aktivitas atau serangan;
   b. *Network enumeration* (menyeleksi jaringan);
   c. Introgasi jaringan;
   d. Mengintai jaringan

   Semua kegiatan ini dapat dilakukan dengan *tools* dan informasi yang tersedia bebas di internet. Kegiatan *footprinting* ini diibaratkan mencari

---

[33] Jogiyanto H.M, *Pengenalan Komputer*, Cetakan Pertama, Andi Ofset, Jogyakarta, 2005, h. 5.

informasi yang tersedia umum melalui buku telepon. *Tools* yang tersedia untuk ini diantaranya :

a) *Teleprot Pro*: Dalam menentukan ruang lingkup, *hacker* dapat men-*download* keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon, *contact person*, dan lain sebagainya.

b) *Whois for* 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (*domain hijack*).

c) *NSLookup*: Mencari hubungan antara *domain name* dengan IP *address*

d) *Traceroute* 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

2) *Scanning* (Pemilihan Sasaran)

Lebih bersifat aktif terhadap sasaran. Di sisni diibaratkan *hacker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan *scanning* dengan demikian dari segi jaringan sangat "berisik" dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali menggunakan *stealth scanning*. *Scanning tool* yang paling legendaris adalah nmap (yang kini sudah tersedia pula untuk *windows* 9x/ME maupun DOS), selain *SuperScan* dan *UltraScan* yang juga banyak digunakan dalam sistem *windows*. Untuk melindungi diri dari kegiatan *scanning* adalah memasang *firewall* seperti misalnya Zone Alarm, atau bila

keseluruhan *network*, dengan menggunakan IDS (*Instrusion Detection Sistem*) seperti misalnya *Snort*.

3) *Enumerasi* (Pencarian Data Mengenai Sasaran)

Sudah bersifat intrusif (mengganggu) terhadap suatu sistem. Di sini penyusup mencari *account name* yang absah, serta *share resources* yang ada. Pada tahap ini, khusus untuk sistem *windows*, terdapat port 139 (NetBIOS *session service*) yang terbuka untuk *resoursce sharing* antar pemakai dalam jaringan. Anda mungkin berpikir bahwa *hard disk* yang di-*share* itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannnya tidak demikian. NetBIOS *session service* dapat dilihat oleh siapapun yang terhubung lewat internet di seluruh dunia! *Tools* seperti *Legion*, SMB *Scanner*, atau *Shares Finder* membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka *resource share tanpa password*).

4) *Gaining Access* (Akses *Illegal* telah didapatkan)

Adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai *user* biasa. Ini adalah kelanjutan dari kegiata *unemerasi*, sehingga biasanya di sini *hacker* sudah mempunyai paling tidak *user account*

5) *Escalating Privilage* (Menaikkan atau Mengamankan Posisi)

Mengasumsikan bahwa penyerang sudah mendapatkan *logon access* pada sistem sebagai *user* biasa. Penyerang kini berusaha naik kelas menjadi admin (pada *sistem windows)* atau menjadi *root* (pada unit *Unix/Linux*). Teknik yang digunakan sudah tidak lagi *dictionary attack* atau *brute force*

attack yang memakan waktu, melainkan mencuri *password file* yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem windows 9x/ME *password* disimpan dalam file. PWL sedangkan pada Windows NT/2000 dalam *file*.SAM. Bahaya pada tahap ini bukan hanya penyerang diluar sistem, melainkan lebih besar lagi bahayanya adalah orang dalam yaitu *user* absah dalam jaringan itu sendiri yang berusaha "naik kelas" menjadi admin atau *root*.

6) Memata-matai data

Pada tahap ini *hacker* mulai melakukan aksinya yaitu *cyber espionage*.

7) Membuat *backdoor* dan menghilangkan jejak

Setelah *hacker* melakukan aksinya, biasanya mereka akan menghilangkan jejak. Seorang *hacker* akan memperkecil kemungkinan terdeteksi oleh orang lain. Cara ini biasanya dengan memanfaatkan *trojan* atau *finger*. "Seorang *hacker* yang berpengalaman, biasanya suatu hari ia akan kembali ke sistem tersebut dan terlalu lama jika prosedurnya atau proses *hacking* diulang dari awal. Berkaitan dengan hal itu biasanya *hacker* membuat *backdoor* atau pintu belakang yang pada dasarnya adalah jalan tembus".[34]

Modus lain dari *cyber espionage* dilakukan dengan metode acak atau tidak sistematis, salah satunya datang dari berita yang menghebohkan dunia dari pusat studi di Kanada, *Munk Center For International Studies*, yang mengemukakan peneliatiannya bahwa adanya sistem komputer mata-mata yang berasal dari Cina yang dapat menyusup kedalam sistem komputer pemerintahan negara di seluruh

[34] Edmon Makarim, *Kompilasi Hukum Telematika*, Cet.2, PT Raja Grafindo Persada, Jakarta, 2004, h. 402.

dunia dan juga instansi data untuk memata-matai data atau informasi untuk kemudian dicuri. Hingga saat ini sedikitnya 103 (seratus tiga) negara yang disusupi dengna jumlah total komputer sebanyak 1295 (seribu dua ratus sembilan puluh lima) unit, kelompok peneliti ini menamakannya *GhostNet*. Cara yang dilakukan pengintai pada kasus ini adalah dengan menyusupkan virus Trojan dan sejumlah *software* jahat yang telah menyusup kedalam sistem komputer dan mengambil dokumen-dokumen yang sifatnya sensitif dari komputer. Laporan riset menyebutkan bahwa sistem komputer mata-mata ini memiliki kemampuan yang luar biasa yang disebut dengan istilah *Big Brother Style*. Selain dapat mencuri data juga dapat membuat komputer yang telah disusupi untuk secara otomatis menyalakan kamera dan menjalankan fungsi rekaman suara untuk tujuan melakukan pengintaian jarak jauh.

Selanjutnya adalah dengan menyusupkan *Spyware*. Istilah *spyware* atau peranti lunak yang memata-matai pengguna komputer telah lama menjadi kosa kata dunia informasi teknologi. *Spyware* merupakan aplikasi yang bertugas untuk melacak aktivitas *surfing* seorang *netter*, *netter* merupakan sebutan untuk orang-orang yang memanfaatkan jaringan internet secara diam-diam. Lalu secara diam-diam pula mengirim informasi-informasi hasil lacakan tersebut ke *server* komputer tertentu yang dirancang oleh si pembuat aplikasi *spyware*. *Spyware* juga dikenal dengan istilah *adware* adalah semacam program tersembunyi yang berfungsi untuk mengirim informasi mengenai komputer yang terinfeksi melalui internet ke si pembuat *spyware*.

Biasanya *spyware* otomatis terinstal baik akibat men*download* sesuatu secara tidak sengaja maupun disususpi secara sengaja oleh orang lain. *Spyware* menjadi berbahaya karena saat ini *spyware* tidak hanya sebagai pengirim info tersembunyi saja, tapi menginstal semacam program khusus yang akhirnya si pemilik *spyware* bisa memata-matai segala aktivitas korban di internet. "Data yang diperoleh dari hasil memata-matai tersebut dikumpulkan dan digunakan untuk kepentingan komersial bahkan kriminal. Tentu saja tanpa seijin dan pengetahuan si *netter*."[35] Hal yang membahayakan lainnya adalah bahwa program pengintai yang bisa mencuri *username* dan *password*, sehingga *spyware* bisa disebut "*species*" baru yang mengancam keamanan komputer setelah virus.

2.3. Perbedaan *Cyber Crime, Cyber Warfare,* dan *Cyber Espionage*

Di dalam dunia maya, banyak jenis operasi siber yang terjadi. Beberapa jenis operasi siber yang paling dikenal adalah *cyber crime, cyber warfare*, dan *cyber espionage*. Masing-masing dari operasi tersebut memiliki unsur berbeda, dan memiliki hukum yang berbeda pula. Maka dari itu, penting untuk mengidentifikasi perbedaan antara operasi-operasi siber sebelum berbicara tentang hukum yang mengaturnya.

> *Cyber crime* atau kejahatan siber diatur dalam *Budapest Convention on Cyber crime*, sebuah konvensi internasional yang dibuka untuk tanda tangan di Budapest, Hongaria pada November 2001, dan berlaku sejak 1 Juli 2004. Konvensi ini dinegosiasikan antara negara anggota Majelis Eropa beserta Kanada, Jepang, Afrika Selatan dan Amerika Serikat, namun terbuka untuk diaksesi negara manapun.[36]

---

[35] Boytra, *Cerita Sedikit Tentang Spyware*, diakses melalui: www.boytra.blogspot.com/2007/08/cerita-sedikit-tentang-spyware.html, diakse pada tanggal 1 Mei 2025.

[36] Hollis, Duncan B., *A Brief Primer on International Law and Cyberspace*, Carnegie Endowment for International Peace, 2021, h. 2.

Konvensi ini mengatur "(i) kriminalisasi perilaku mulai dari akses ilegal, gangguan data dan sistem hingga penipuan terkait komputer dan pornografi anak; (ii) perangkat hukum acara untuk menyelidiki kejahatan dunia maya dan mengamankan bukti elektronik terkait dengan kejahatan apapun; dan (iii) kerjasama internasional yang efisien".[37] Menurut Pasal 13 ayat (1). Konvensi ini mengharuskan setiap Pihak untuk menerapkan Undang-Undang yang mengkriminalisasi pelanggaran-pelanggaran melalui komputer yang diatur dalam Pasal 2 hingga Pasal 11. Pelanggaran yang tertulis dalam Pasal-Pasal tersebut antara lain:

1) Akses ilegal;
2) Penyadapan ilegal;
3) Gangguan data;
4) Gangguan sistem;
5) Penyalahgunaan perangkat;
6) Pemalsuan yang berhubungan dengan komputer;
7) Penipuan yang berhubungan dengan komputer;
8) Pelanggaran yang berkaitan dengan pornografi anak;
9) Pelanggaran yang berkaitan dengan hak cipta dan hak-hak lainnya;
10) Mencoba dan menolong atau bersekongkol; dan
11) Pertanggungjawaban perusahaan.

Cyber crime tidak memiliki satu definisi hukum yang pasti, namun dapat disimpulkan dari unsur-unsur yang ada di dalam konvensi yang mengaturnya. Jika

[37] Majelis Eropa, *The Budapest Convention on Cyber Crime: Benefits and Impact in Practice Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, diakse pada tanggal 1 Mei 2025.

mengacu pada jenis-jenis pelanggaran yang diatur dalam *Budapest Convention on Cyber crime*, dapat dilihat bahwa masing-masing pelanggaran tersebut merupakan pelanggaran yang dilakukan melalui dunia maya. Menurut Pasal 14 ayat (2), selain dari pelanggaran yang tertulis dalam Pasal 2 hingga Pasal 11, langkah-langkah legislatif juga dapat diterapkan pada tindak pidana lain yang dilakukan melalui sistem komputer. Maka dari itu, dapat disimpulkan bahwa definisi *cyber crime* atau kejahatan siber adalah kejahatan yang berkaitan dengan sistem komputer atau dilakukan di dunia maya.

> Di dalam pembukaan *Budapest Convention on Cyber crime*, perancang konvensi mengingat kembali konvensi lain serta rekomendasi mengenai perlindungan data pribadi, salah satunya *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (disebut juga *Convention ETS* (*European Treaty Series*) 108) yang juga dirancang oleh Majelis Eropa. Data pribadi dalam konteks *Budapest Convention on Cyber Crime* dibahas dalam salah satu laporan Majelis Eropa, *Cyber Crime Investigation and the Protection of Personal Data and Privacy*. Menurut dokumen tersebut, *Budapest Convention on Cyber Crime* mengacu pada *Convention* ETS 108 tentang data pribadi, walaupun di dalam *Cyber Crime Convention* sendiri tidak tertulis definisi data pribadi.[38]

Jika melihat dari tujuan dokumen dan filosofi yang tertuang di pembukaan *Cyber Crime Convention*, serta konvensi dan rekomendasi yang dijadikan acuan, dapat ditarik kesimpulan bahwa data yang menjadi target dalam *cyber crime* lebih merujuk kepada data pribadi. Selain *cyber crime*, jenis operasi siber lain adalah *cyber warfare*. "Istilah *cyber warfare* atau perang dunia maya mengacu pada cara dan metode peperangan yang terdiri dari operasi siber yang berujung pada, atau

---

[38] Majelis Eropa, ***C****ybercrime Investigation and The Protection of Personal Data and Privacy Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, diakses pada tanggal 1 Mei 2025.

dilakukan dalam, konteks konflik bersenjata sesuai dengan pengertian di dalam Hukum Humaniter Internasional (HHI)".[39]

Selain *Budapest Convention on Cyber Crime* dan *African Union Convention on Cyber Security and Personal Data Protection* yang belum berlaku, belum ada aturan khusus yang mengatur aktivitas di *cyber space*. *Cyber warfare* tidak diatur di dalam perjanjian internasional khusus, namun tetap diatur di bawah hukum humaniter internasional, karena dilakukan di dalam konteks konflik bersenjata. Serangan siber yang dilakukan dalam *cyber warfare* berpotensi untuk memiliki dampak humaniter. Ketika komputer atau jaringan suatu Negara diserang, disusupi, atau diblokir, mungkin ada risiko warga sipil kehilangan kebutuhan dasar seperti listrik, air minum, dan perawatan medis. "Menurut ICRC, aturan dan batasan perang berlaku pada *cyber warfare* seperti halnya dengan penggunaan senapan, artileri, dan misil".[40]

Operasi siber selanjutnya adalah *cyber espionage*, yang telah dibahas di bagian kedua kajian pustaka. Seperti kebanyakan aktivitas yang dilakukan di dunia maya, *cyber espionage* belum diatur oleh perjanjian khusus dalam hukum internasional, sehingga belum memiliki satu definisi yang pasti. Jika merujuk pada definisi tindakan illegal interception dalam *Budapest Convention on Cyber Crime*, dapat dibuat argumentasi bahwa *cyber espionage* merupakan bagian dari *cyber crime*.

> Menurut para ahli Tallinn Manual 2.0, *cyber espionage* dapat didefinisikan sebagai, "*any act undertaken clandestinely or under false pretences that*

---

[39] ICRC (*International Committee of the Red Cross*), *Cyber Warfare and International Humanitarian Law: The ICRC's Position*, diakses melalui: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf, diakses pada tanggal 1 Mei 2025.

[40] *Ibid*.

> *uses cyber capabilities to gather, or attempt to gather, information,"* yang berarti setiap tindakan yang dilakukan secara sembunyi-sembunyi atau dengan alasan palsu menggunakan kemampuan dunia maya untuk mengumpulkan (atau berusaha mengumpulkan) informasi.[41]

Definisi tersebut memiliki unsur-unsur yang sama dengan definisi spionase yang tertulis dalam Deklarasi Brussels 1874, serta Konvensi Den Haag 1899 dan 1907, di mana selalu tertulis kriteria "*acting clandestinely or on false pretences, he obtains or endeavours to obtain information*." Satu-satunya hal yang membedakan definisi spionase biasa dengan *cyber espionage* adalah unsur pengambilan informasi melalui dunia maya.

"*Cyber espionage* sering kali dibedakan menjadi dua kategori, yaitu *political* dan *economic cyber espionage*, berdasarkan informasi yang diambil".[42] Dalam konteks ini, informasi yang diambil merupakan milik negara lain, dilakukan untuk mendapat keuntungan politik atau ekonomi. Hal ini yang mungkin membedakan *cyber espionage* dengan *cyber crime* seperti dimaksud dalam *Budapest Convention on Cyber Crime*; di mana *cyber crime* cenderung berhubungan dengan data pribadi, *cyber espionage* berhubungan dengan informasi rahasia atau sensitif milik suatu negara.

2.4. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia telah mengatur hubungan-hubungan hukum tentang kejahatan yang berkaitan dengan komputer (*komputer crime*) yang kemudian berkembang menjadi *cyber crime*. Dasar pokok

---

[41] International Groups of Experts at the Invitation of the NATO CCDCOE, *Tallinn Manual 2.0*, Cambridge University Press, Cambridge, 2017, h. 168.

[42] Herrmann, Dominik, *Cyber Espionage and Cyber Defence*, *Information Technology for Peace and Security*, Springer Vieweg, Wiesbaden, 2019, h. 84.

dalam menjatuhkan pidana atas pelaku *cyber espionage* di Indonesia, harus memenuhi kualifikasi perbuatan pidana. Mengingat *cyber espionage* merupakan salah satu aktvitas *cyber crime* yang dilakukan oleh *hacker*, yang merupakan kejahatan terhadap informasi seseorang, instansi ataupun lembaga yang bersifat pribadi dan rahasia sehingga penerapan Pasal-Pasal pidana haruslah tepat baik berdasarkan yang ada dalam KUHP maupun diluar KUHP karena kegiatan mata-mata ini melalui proses yang runtut.

> Moeljatno dalam bukunya tentang "Asas-asas Hukum Pidana Di Indonesia" dikatakan bahwa, untuk dapat digolongkan menjadi suatu perbuatan pidana, maka suatu perbuatan itu harus terlebih dulu dilarang dan diancam dengan pidana dalam suatu perundang-undangan yang berlaku. Persyaratan pemidanaan ini dikenal dengan sebutan asas legalitas (*principle of legality*). Dalam bahasa Latin dikenal dengan "*Nullum Delictum nulla poen sine preaviaa lege*" dan dalam bahasa Indonesia diterjemahkan sebagai tiada delik, tiada pidana tanpa peraturan lebih dahulu atau dengan kalimat sederhana "tiada suatu perbuatan yang dapat dipidana selain telah ada ketentuan-ketentuan perundang-undangan pidana yang mendahuluinya".[43]

Lebih lanjut Moeljatno menambahkan bahwa penerapan asas legalitas dalam hukum pidana Indonesia mengandung 3 (tiga) pengertian yaitu:[44]

a. Suatu perbuatan tidak dapat dipidana kalau terhadap perbuatan itu tidak ada ketentuan perundang-undangan yang mengaturnya. Hal ini nampak jelas dalam ketentuan Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana yang berbunyi: "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelum perbutan dilakukan".
b. Tidak boleh menggunakan analogi dalam menentukan adanya suatu perbuatan pidana. Suatu analogi terhadap aturan hukum pidana dilarang karena analogi bersifat subjektif, tidak berpegang pada aturan yang ada tetapi menggunakan ratio terhadap maksud dan inti dari aturan yang ada sehingga dapat berakibat pada ketidakadilan dalam suatu putusan pengadilan.
c. Tidak berlakunya asas retroaktif (berlaku surut) terhadap aturan-aturan hukum pidana. Namun dalam perkembangan akhir-akhir ini, telah

---

[43] Moeljatno, *Asas-Asas Hukum Pidana*, Cet.VII, Rineka Cipta, Jakarta, 2002, h. 23.
[44] *Ibid*, h. 25.

diperbolehkan berlakunya asas retroaktif ini dalam batas-batas tertentu seperti terhadap pelaku kejahatan/pelanggaran Hak Asasi Manusia berat.

Berdasarkan persyaratan asas legalitas ini maka pemidanaan terhadap pelaku *cyber espionage* tentunya harus didasarkan pada sumber hukum yang berlaku saat ini yakni Kitab Undang-Undang Hukum Pidana maupun peraturan perundang-undangan lain diluar Kitab Undang-Undang Hukum Pidana yang berkaitan dengan *cyber espionage*.

Dalam hukum pidana terdapat pendekatan dalam menerapkan suatu ketentuan pidana, yang biasa dikenal dengan istilah interpretasi atau penafsiran. Tidak akan diuraikan secara menyeluruh mengenai penafsiran, namun secara lebih khusus akan akan dibahas mengenai penafsiran ekstensif. Penafsiran ekstensif adalah memperluas pengertian dari suatu istilah berbeda dengan pengertiannya yang digunakan dalam istilah sehari-hari. Mengenai penggunaan cara penafsiran ini sering terjadi perbedaan pendapat diantara para sarjana karena sukar memberi batas bagi perluasan tersebut. Hal ini menjadi perhatian karena analogi juga dikatakan sebagai perluasan pengertian atau perluasan cakupan ketentuan suatu peraturan, padahal pada umumnya analogi tidak diperbolehkan dalam hukum pidana.

Menggunakan analogi berarti menganggap sesuatu sebagai termasuk dalam pengertian dari suatu ketentuan Undang-Undang hukum pidana, karena sesuatu itu banyak sekali kemiripannya atas kesamaannya dengan ketentuan tersebut. Contoh terkenal mengenai penerapan analogi adalah kasus pencurian aliran listrik. Yang menjadi persoalan adalah, apakah aliran listrik dianggap sebagai “barang” dan apakah terjadi terjadi tindakan “mengambil”. Hooge Raad (Mahkamah Agung

negara Belanda) telah memutuskan bahwa aliran listrik termasuk dalam pengertian barang dan dengan demikian terjadi pengambilan sesuai denagan istilah yang digunakan Pasal 362 Kitab Undang-Undang Hukum Pidana, walaupun pada kenyataannya yang terjadi adalah penyalurannya. "Pertimbangan Hoge Raad adalah, bahwa maksud dari Pasal 362 adalah untuk melindungi harta orang lain, tanpa merumuskan apa yang dimaksud dengan barang. (Arrest HR tanggal 23 Mei 1921 W.10728)".[45]

Penafsiran ekstensif berbeda dengan analogi, menurut Wirjono perbedaan antara penafsiran ekstensif dengan analogi adalah : Orang masih ada di bidang penafsiran ekstensif apabila dari kata-kata suatu peraturan hukum tidak terlihat, tetapi dengan suatu cara pikiran itu disimpulkan, bahwa suatu kejadian atau peristiwa tertentu dimaksudkan turut teratur juga. "Sedangkan analogi terjadi apabila suatu penafsiran disimpulkan bahwa suatu kejadian atau peristiwa tertentu tidak turut diatur dalam suatu peraturan hukum, namun tetap saja dianggap diliputi oleh peraturan itu".[46]

Penerapan Kitab Undang-Undang Hukum Pidana terhadap tindak pidana *cyber espionage* memerlukan pemilah-milahan, perbuatan yang mana substansinya hampir sama dengan rumusan tindak pidana biasa dalam Kitab Undang-Undang Hukum Pidana, rumusan perbuatan *cyber espionage* adalah merupakan kejahatan yang menggunakan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain. Dengan memasuki jaringan komputer

---

[45] E.Y. Kanter dan S.R Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, Alumni AHM-PTHM, Jakarta, 1982, h. 76.

[46] Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana Indonesia*, PT Eresco, Jakarta, 1969, h. 68.

(*komputer network sistem)* pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen maupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*. Mengingat *cyber espionage* melalui proses yang runtut, maka penjatuhan pidana didasarkan pada relevansi tindak pidana yang dilakukan dari awal hingga akhir, sehingga Pasal yang dijerat pun bisa lebih dari 1 (satu).

Berdasarkana penjelasan mengenai modus operandi *cyber espionage* pada bab sebelumnya, maka ada beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana yang dapat dikenakan terhadap pelaku, diantaranya adalah aturan yang mengatur perihal ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain yaitu dalam Pasal 167 Kitab Undang-Undang Hukum Pidana, yang rumusannya sebagai berikut:

Pasal 167

1) Barang siapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau paling banyak empat ribu lima ratus rupiah.
2) Barang siapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu, atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karna kekhilafan masuk dan kedapatandi situ pada waktu malam, dianggap memaksa masuk.
3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan.
4) Pidana tersebut dalam ayat (1) dan ayat (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Sebagaimana kita ketahui bahwa konvergensi teknologi (komputer, komunikasi dan informasi), yang terwujud dalam bentuk internet, dimana isu privasi merupakan suatu hal yang tidak bisa ditawar lagi. Jika terjadi suatu

penuyusupan terhadap suatu sistem komputer dan disaat yang bersamaan tindakan tersebut telah terdeteksi oleh pemilik sistem, tindakan tersebut dapat dikategorikan sebagai suat kejahatan jika dampak yang ditimbulkan menimbulkan kerugian pada orang lain. Unsur-unsur yang dapat ditemukan dalam Pasal 167 Kitab Undang-Undang Hukum Pidana sebagai berikut:

1) Unsur Subjektif

Unsur subjektif yang dimaksud dengan Pasal 167 Kitab Undang-Undang Hukum Pidana adalah tiada kekhilafan atau ringkasnya adanya suatu kesengajaan dalam melakukan perbuatan tersebut. Jika kita kembali melihat Kitab Undang-Undang Hukum Pidana (R.Sesilo), perbuatan tersebut dilakukan dengan kesengajaan, dimana pelaku terdeteksi (diketahui) dan setelah diperingati tidak dihindarkan oleh yang bersangkutan. Dari rumusan tersebut kiranya dapat ditarik kesimpulan bahwa adanya suatu kesengajaan dalam tindakan tersebut. Jika Kitab Undang-Undang Hukum Pidana diterapkan dalam *cyber espionage* ini, maka sifat kesengajaan dari perbuatan tersebut perlu dibuktikan di siding pengadilan, dan jika terbukti maka pelaku (*hacker*) baru dapat dipidana. Kesengajaan menurut doktin dalam hukum pidana terbagi atas:[47]

a. Kesengajaan sebagai maksud atau tujuan. Yakni terjadinya suatu tindakan atau maksud atau akibat tertentu (sesuai dengan perumusan Undang-Undang Hukum Pidana) kesengajaan dengan kesadaran kepastian atau keharusan
b. Seberapa jauh pengetahun atau kesadarn pelaku tentang tindakan dan akibat yang merupakan salah satu unsur dari pelaku delik. Disini termasuk tindakan atau akibat tersebut harus pasti terjadi.

---

[47] Edmon Makarim, *Kompilasi Hukum Telematika*, Cet.2, PT Raja Grafindo Persada, Jakarta, 2004, h. 409.

c. Kesengajaan dengan kesadaran kemungkinan, yakni kesengajaan dengan gradasi terendah, bahkan sering sukar untuk membedakan dengan culpa, yang menjadi sandaran adalah sejauh mana pengetahuan atau pelaku, tentang akibat dan tindakan yang dilarang beserta tindakan lainnya yang mungkin akan terjadi.

2) Unsur Objektif

Memasuki wilayah dalam hal ini wilayah fisik (rumah, ruangan, pekarangan tertutup). Sifat fisik ini yang membatasi aturan pidana Kitab Undang-Undang Hukum Pidana dapat diterapkan, *cyber space* bukanlah wilayah fisik seperti yang kita bayangkan. Oleh sebab itu perlu adanya perubahan makna, jangan lagi sifat fisik dari *cyber space* diajdikan perdebatan, tetapi pada "tindakan atau perbuatan masuk melawan hukumnya." Dunia maya (*cyber space*) yang bersifat tidak nyata ini menjadikan tindakan yang bersifat fisik tidak lagi dijadikan sandaran bahwa pelaku telah melakukan tindak pidana. Unsur barangsiapa tetap dijadikan patokan, hanya cara yang dilakukantidak lagi langsung pada objek fisik, tindakan yang dimaksud disini berupa suatu jejak elektronik (*electronic path*) yang berisikan *log file*, angka atau data matematis yang mengindikasikan telah berlangsung aktivitas elektronik.

Pasal lain yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 Kitab Undang-Undang Hukum Pidana, yang berbunyi: Barang siapa tanpa wewenang berjalan atau berkendaraan dia atas tanah yang oleh pemiliknya dengan cara jelas dilarang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah.

Jika dilihat dari susunan kata perkatanya saja, kesimpulan yang dapat ditarik dari Pasal ini adalah bahwa Pasal ini melarang orang yang berjalan atau berkendaraan di atas tanah orang lain yang nyata-nyata sudah diberi tanda larangan bahwa tanah itu tidak boleh dilalui. Namun demikian, apabila dilakukan kajian perluasan konsepsi, tanah identik dengan ruang atau fasilitas sistem komputer karena memiliki kesamaan sifat yaitu properti. Berjalan atau berkendara di atas tanah tanpa ijin meski sudah ada larangan dapat disamakan sebagai akses kepada fasilitas komputer tanpa ijin. Penggunaan *user-id*, *password* dan alat verifikasi lainnya dapat disamakan sebagai alat masuk tanpa ijin.

Berkaitan dengan Pasal diatas, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanganan hukum siber jenis *cyber espionage* yang sangat ringan (dapat mengganti pidaan kurungan) padahal *cyber espionage* yang umumnya terjadi dapat merugikan financial yang tidak sedikit.

Apabila berhubungan dengan kaamanan negara, Kitab Undang-Undang Hukum Pidana hannya mengatur spionase terhadap negara yang cenderung dilakukan secara konvensional pada saat perang, yakni terdapat dalam Pasal 124 ayat (2) dan 126 Kitab Undang-Undang Hukum Pidana. Pada Pasal 124 ayat (2) Kitab Undang-Undang Hukum Pidana dirumuskan bahwa:

Pasal 124 ayat (2)

Diancam dengan pidana penjara seumur hidup atau selama waktu tertentu atau paling lama dua puluh tahun jika si pembuat:

1. Memberitahukan atau memberikan kepada musuh peta, rencana, gambar, atau penulisan mengenai bangunan-bangunan tentara;
2. menjadi mata-mata musuh, atau memberikan pondokan kepadanya.

Ketentuan lain yang berkaitan dengan tindak pidana *cyber espionage* apabila perbuatan seseorang itu menyangkut bocornya data keluar terutama

mengenai data yang harus dirahasiakan (*data leakage*) maka ketentuan yang dapat diterapkan adalah ketentuan yang berkaitan dengan perbuatan membocorkan suatu rahasia. Ketentuan yang berkaita dengan membcorkan suatu rahasia negara (termasuk di dalamnya perbuatan dengan menggunakan sarana internet) diatur dalam Pasal 112, Pasal 113 dan Pasal 114 Kitab Undang-Undang Hukum Pidana serta perbuatan yang membocorkan rahasia perusahaan yang diatur dalam Pasal 322 dan Pasal 323 Kitab Undang-Undang Hukum Pidana.

Pasal 112

> Barang siapa dengan sengaja mengumumkan surat-surat, berita-berita atau keterangan- keterangan yang diketahuinya bahwa harus dirahasiakan untuk kepentingan negara, atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun.

Pasal 113

1) Barang siapa dengan sengaja, untuk seluruhnya atau sebagian mengumumkan, atau memberitahukan maupun menyerahkan kepada orang yang tidak berwenang mengetahui, surat-surat, peta-peta, rencana-rencana, gambar-gambar atau benda benda yang bersifat rahasia yang bersangkutan dengan pertahanan atau keamanan Indonesia terhadap serangan dari luar, yang ada padanya atau yang isinya, bentuknya atau susunanya benda- benda itu diketahui olehnya, diancam dengan pidana penjara paling lama empat tahun.
2) Jika surat-surat atau benda-benda ada pada yang bersalah, atau pengetahuannya tentang itu karena pencariannya, pidananya dapat ditambah sepertiga.

Pasal 114

> Barang siapa karena kesalahannya (kealpaannya) menyebabkan surat-surat atau benda- benda rahasia sebagaimana yang dimaksudkan dalam Pasal 113 harus menjadi tugasnya untuk menyimpan atau menaruhnya, bentuk atau susunannya atau seluruh atau sebagian diketahui oleh umum atau dikuasai atau diketahui oleh orang lain (atau) tidak berwenang mengetahui, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana kurungan paling lama satu tahun atau pidana denda paling tinggi empat ribu lima ratus rupiah.

Pasal ini merupakan ketentuan yang berkaitan dengan perbuatan pembocoran rahasia negara yang sering kali bersinggunangan dengan masalah spionase. Kaitannya dengan kejahatan siber khususnya dengan *cyber espionage* adalah pembukaan rahasia negara dapat dilakukan kepada pihak yang tidak berwenang untuk menerima rahasia tersebut. Untuk masuk dalam suatu terminal yang berisikan rahasia negara memang dibutuhkan suatu keahlian khusus tetapi bukan berarti hal yang tidak mungkin dapat dilakukan karena basis data pemerintah saat ini banyak yang menggunakan kecanggihan teknologi *e-government*. Unsur kesengajaan pada Pasal 1 ini diancam pidana paling lama 7 (tujuh) tahun.

Sedangkan membocorkan rahasia perusahaan dapat dikaterorikan sebagai kejahatan membuka rahasia, sehingga si pelaku dapat diancam dengan pidana berdasarkan Pasal 322 dan Pasal 323 Kitab Undang-Undang Hukum Pidana.

Pasal 322

1) Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah.
2) Jika kejahatan dilakukan terhadap seorang tertentu, maka perbuatan itu hanya dapat dituntut atas pengaduan orang itu.

Pasal 323

1) Barang siapa dengan sengaja memberitahukan hal-hal khusus tentang suatu perusahaan dagang, kerajinan atau pertanian, di mana ia bekerja atau dahulu bekerja, yang harus dirahasiakannya, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah.
2) Kejahatan ini hanya dituntut atas pengaduan pengurus perusahaan itu.

Perkembangan teknologi informasi bagi kegiatan suatu negara ataupun perusahaan seperti menyimpan surat-surat atau menyimpan benda-benda rahasia ke dalam *data base* atau *storage* yang berupa data merupakan suatu sisi positif

dari dari kehadiran teknologi informasi itu sendiri. Suatu data dapat juga mengenai organisasi kenegaraan atau produksi mengenai metode dan bahan baku serta angka produksi perusahaan dan sebagainya. Tetapi manakala data ini jatuh ke pihak ketiga yang tidak berwenang untuk menerima, mengetahui atau mendapatkannya maka hal tersebut dapat merugikan dan membahayakan bagi kelangsungan dari perusahaan yang bersangkutan.

Selain sanksi pidana yang dikenakan untuk delik atau tindak pidana yang telah selesai dilakukan, Kitab Undang-Undang Hukum Pidana juga mengatur mengenai percobaan kejahatan tindak pidana sebagaimana yang tertulis pada Pasal 53 (1) Kitab Undang-Undang Hukum Pidana yang berbunyi: " Mencoba melakukan kejahatan dipidana, jika niat untuk itu telah ternyata dari adanya permulaan pelaksanaan, dan tidak selesainya pelaksanaan itu, bukan semata-mata disebabkan karena kehendaknya sendiri". Unsur-unsur yang pada Pasal tersebut adalah : 1) adanya niat; 2) adanya permulaan pelaksanaan; 3) tidak selesainya tindak kejahatan tersebut bukan karena kehendaknya sendiri

Pasal tersebut apabila dikatkan dengan tindak pidana di bidang teknologi informasi khususnya tindak pidana *cyber espionage*, maka relevansinya adalah apabila pelaku atau *hacker* berdasarkan modus operandi sebagaimana telah dijelaskan pada bab sebelumnya telah berhasil memasuki akses jaringan internet atau komputer milik pihak lain dengan niat untuk memata-matai data dengan didahului kegiatan pencariaan data (*footprinting*), pemilihan sasaran (*scanning*) dan/atau pencarian data mengenai sasaran (*enumerasi*), namun belum sampai pada tahap *cyber espionage* atau memata-matai data bukan karena kehendaknya

sendiri, maka pelaku dapat dikenakan Pasal ini karena spionase sendiri merupakan tindak pidana kejahatan bukan pelanggaran.

2.5. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik

Tindak pidana *cyber espionage* ini merupakan Tindak Pidana khusus yang artinya dari segi hukum materiilnya menyimpangi Kitab Undang-Undang Hukum Pidana (KUHP), sedangkan dari sisi hukum formilnya masih mengikuti ketentuan yang ada dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sebelum disahkannya Undang-Undang Informasi dan Transaksi Elektronik, penanganan atas tindak pidana *cyber espionage* belum mendapat payung hukum yang jelas. Hal ini disebabkan belum ada satupun Undang-Undang yang mengatur tentang tindak pidana *cyber espionage* secara eksplisit. Kitab Undang-Undang Hukum Pidana hanya mengatur tentang tindak pidana spionase konvensional dan tindak pidana-tindak pidana yang dapat ditafsirkan secara ektensif sebagai tindak pidana *cyber espionage*.

Penggunaan Pasal-Pasal yang sudah tidak sesuai lagi atau dapat dikatakan kurang tepat dapat menyulitkan aparat dalam menjerat pelaku, tidak saja dikarenakan hukum materiilnya yang tidak mengakomodir bentuk baru dari kejahatan spionase atau mata-mata ini, tetapi juga hukum formil yang bersumber dari Kitab Undang-Undang Hukum Acara Pidana belum mengenal adanya alat bukti digital. Padahal sebagian besar barang bukti yang didapat dari penyidikan tindak pidana *cyber espionage* berbentuk digital. Secara yuridis kegiatan *cyber space* tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional

saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.

Setelah disahkannya Undang-Undang informasi dan transaksi elektronik ini maka terbentuklah payung hukum para aparat penegak hukum untuk menangkap dan menjerat pelaku kejahatan ini. Manfaat yang dapat diambil dengan adanya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah: 1) Menjamin kepastian hukum bagi masyarakat; 2) Mendorong pertumbuhan ekonomi; 3) Sebagai salah satu upaya untuk mencegah terjadinya kejahatan berbasis teknologi informasi; dan 4) Melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi.

Di dalam Undang-Undang Informasi dan Transaksi Elektronik, *cyber espionage* diatur dalam Pasal 30 ayat (2) yang berbunyi: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen Elektronik dikenai sanksi pidana berdasarkan Pasal 46 ayat (2) yang berbunyi: Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).

Hacker yang melakukan aksi mata-mata atau *cyber espionage* untuk mendapatkan informasi dari hasil mengakses komputer secara *illegal* memenuhi unsur-unsur yang ada dalam rumusan Pasal 30 ayat (2) Undang-Undang ini. Sedangkan untuk orang (*hacker*) yang dengan sengaja memfasilitasi orang lain

agar bisa mengetahui ataupun mengakses informasi yang bukan haknya sebagaimana yang terjadi pada kasus pembuat *Spyware* jenis *Lover Spy*, maka dapat dikenakan Pasal 32 ayat (2) dan Pasal 34 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yakni: Setiap orang dengan sengaja dan tanpa hak atau melawan hukumdengan cara apa pun memindahkan atau mentrasfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.

Pasal 34 ayat (1):

> Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untukm digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
>
> a. Perangkat keras atau perangkat lunak computer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
> b. Sandi lewat computer, kode akses, atau hal yang sejenis dengan ituyang ditujukan agar system Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Undang-Undang Informasi dan Transaksi Elektronik selain mengatur mengenai tindak pidana terhadap perbuatan *cyber espionage* itu sendiri, juga mengatur mengenai subjek yang melakukan tindak pidana tersebut, yankni yang dilakukan oleh perorangan maupun oleh korporasi. Adanya pengaturan tersebut berimplikasi pada pidana yang akan dijatuhkan, sebagaimana yang tercantum pada Pasal 52 ayat (4) yakni : "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua per tiga".

Mengenai percobaan, Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur secara tersendiri, oleh sebab itulah maka secara otomatis berlaku

ketentuan Pasal 86 Kitab Undang-Undang Hukum Pidana. Berdasarkan Pasal 86 Kitab Undang-Undang Hukum Pidana, maka jika di dalam suatu Undang-Undang diatur tentang tindak pidana kejahatan didalamnya termasuk ketentuan tentang percobaan. Dengan dmikian, meskipun Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur tentang percobaan, maka siapapun yang mencoba melakukan tindak pidana di bidang Informasi dan Transaksi Elektronik, akan tetap dijatuhi pidana dengan ancaman maksimum pidana pokok dikurangi sepertiga. Hal ini sesuai dengan Pasal 53 dan Pasal 56 Kitab Undang-Undang Hukum Pidana.

Berbeda dengan Percobaan yang masih menggunakan ketentuan yang ada dalam Kitab UndangUndang Hukum Pidana, hal lain yang diatur secara khusus pada Undang-Undang Informasi dan Transaksi Elektronik adalah mengenai hukum acara formil atas tindak pidana siber (*cyber crime*). Terutama mengenai alat bukti yang digunakan dalam tindak pidana siber ini. Hal ini berdasarkan Pasal 44 yang berbunyi :

Pasal 44

Alat bukti penyidikan, penuntutan, dan pemerikasaan di siding pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
b. Alat bukti berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angkan 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

2.6. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Undang-Undang Telekomunikasi

Di bidang komunikasi yang merupakan bagian dari teknologi komunikasi, ketentuan yang mengatur tentang tindak pidana kejahatan telekomunikasi sudah

diatur dalam Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang berbunyi: “Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atua memanipulasi: a) Akses ke jaringan telekomunikasi; dan atau b) Akses ke jasa telekomunikasi; dan atau c) Akses atau jaringan ke telekomunikasi khusus”.

Unsur-unsur dalan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi antara lain: a) Setiap orang; b) Dilarang; c) Melakukan perbuatan tanpa hak; d) Tidak sah; e) Memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi dan atau akses ke jaringan telekomuniksi khusus. Pada Pasal ini tidak tidak secara langsung menggunakan kata cyber espionage dalam rumusan Pasalnya, tetapi mengatur mengenai akses tidak sah ,sehingga aksi *hacker* yang melakukan spionase untuk mengintai atau memata-matai data melanggar ketentuan Pasal ini.

Penekanan dari Pasal ini adalah larangan terhadap akses tidak sah kepada jaringan dan jasa telekomunikasi. Pada kenyataannya dan sesuai dengan definisi telekomunikasi (Pasal 1 Undang-Undang Nomor 36 Tahun 1999) tidak ada perbedaan lagi antara jaringan dan jasa telekomunikasi dengan jaringan dan jasa teknologi informasi, karena di dalamnya juga selalu ada jaringan komputer. Oleh karena itu tindakan mengakses sistem komputer dengan tidak sah dapat dikenai tuntutan pidana sebagaimana dimaksud dalam Pasal 50 yang berbunyi: “Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda peling banyak Rp.600.000.000,- (enam ratus juta rupiah)”.

Penekanan sanksi pidana pada pelanggar akses tidak sah, dengan tuntutan pidana penjara serta denda sesuai dengan Pasal 50, menguatkan pentingnya jaminan keamanan terhadap data-data yang secara *computerized* patut untuk dilindungi, sehingga tindakan apapun yang dilakukan *hacker* pada sebuah jaringan komputer khusunya internet tanpa kewenangan patut ditindak secara tegas.

2.7. Pengaturan Kejahatan *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia

Pengaturan kejahatan *cyber espionage* berdasarkan hukum positif yang ada di Indonesia menunjukkan bahwa regulasi yang tersedia masih bersifat umum dan belum secara spesifik mengatur jenis kejahatan ini. *Cyber espionage*, atau spionase siber, adalah tindakan memperoleh data rahasia melalui jaringan komputer tanpa izin, biasanya untuk kepentingan politik, militer, atau ekonomi.

> Menurut Prof. Barda Nawawi Arief menyatakan bahwa *cyber* atau siber merupakan suatu istilah untuk menjelaskannya dengan istilah "mayantara". *Cyber* juga dapat diartikan dari bahasa Inggris sebagai suatu istilah "maya, tidak nyata, tidak terlihat, terawang, terawang, tidak ada bentuk". Dengan mengartikan *cyber espionage* dalam penjelasan yang lebih komprehensif, perlu juga di maknai apa itu spionase dan elemen-elemen yang menjadi parameter dalam tindakan spionase.[48]

Di Indonesia, pengaturan terkait kejahatan ini secara tidak langsung dapat ditemukan dalam beberapa peraturan, namun belum mencakup secara komprehensif. Diantaranya sebagai berikut:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, menjadi dasar hukum utama dalam menindak kejahatan

[48] Aldo Rahmandana, *Tinjauan Yuridis Cyber Espionage Berdasarkan Hukum Internasional*, Jurnal Jurist-Diction, Vol.4, No.6, 2021, h. 2143.

berbasis teknologi informasi. Namun, Undang-Undang Informasi dan Transaksi Elektronik lebih fokus pada akses ilegal, penyadapan, perusakan sistem elektronik, dan pencurian data, tanpa secara eksplisit mengatur tindakan *cyber espionage* yang melibatkan spionase terhadap negara atau perusahaan.

2. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memuat larangan terhadap tindakan yang mengancam keamanan negara, termasuk kegiatan spionase, tetapi tidak memberikan rincian mengenai bentuk kejahatan siber sebagai salah satu modus spionase.
3. Kitab Undang-Undang Hukum Pidana sendiri belum secara memadai mengatur kejahatan siber, karena merupakan produk hukum yang lahir sebelum era digital. Beberapa Pasal tentang pengkhianatan atau pencurian informasi negara memang ada, namun tidak relevan dengan karakteristik *cyber espionage* modern yang sering dilakukan secara anonim dan melintasi batas negara.
4. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme pun belum menyentuh ranah spionase siber, meskipun dapat terkait secara tidak langsung bila *cyber espionage* digunakan untuk kepentingan aksi terorisme.

Dengan demikian, analisa terhadap hukum positif yang ada menunjukkan adanya kekosongan normatif dan belum adanya regulasi khusus yang secara tegas dan terperinci mengatur *cyber espionage* sebagai tindak pidana tersendiri. Untuk menjamin kepastian hukum dan efektivitas penegakan hukum terhadap kejahatan

ini, dibutuhkan pembaruan hukum, baik melalui revisi Undang-Undang yang ada maupun pembentukan instrumen hukum baru yang spesifik mengatur kejahatan siber lintas negara dan berdimensi intelijen seperti *cyber espionage*.

BAB III

PERTANGGUNGJAWABAN PELAKU TINDAK PIDANA *CYBER ESPIONAGE* BERDASARKAN HUKUM POSITIF DI INDONESIA

3.1. Pertanggungjawaban Hukum

Pertanggungjawaban hukum berkaitan erat dengan konsep hak dan kewajiban. Konsep hak merupakan suatu konsep yang menekankan pada pengertian hak yang berpasangan dengan pengertian kewajiban. Pendapat yang umum mengatakan bahwa hak pada seseorang senantiasa berkorelasi dengan kewajiban pada orang lain. Sebuah konsep yang berkaitan dengan konsep kewajiban hukum adalah konsep tanggung jawab hukum. Bahwa seseorang bertanggung jawab secara hukum atas perbuatan tertentu atau bahwa dia memikul tanggung jawab hukum, artinya dia bertanggung jawab atas suatu sanksi bila perbuatannya bertentangan dengan peraturan yang berlaku.

"Menurut Hans Kelsen dalam teorinya tentang tanggung jawab hukum menyatakan bahwa seseorang bertanggung jawab secara hukum atas suatu perbuatan tertentu atau bahwa dia memikul tanggung jawab hukum, subjek berarti bahwa dia bertanggung jawab atas suatu sanksi dalam hal perbuatan yang bertentangan".[49] Suatu konsep terkait dengan konsep kewajiban hukum adalah konsep tanggung jawab hukum (*liability*). "Seseorang dikatakan secara hukum bertanggung jawab untuk suatu perbuatan tertentu adalah bahwa dia dapat dikenakan suatu sanksi dalam kasus perbuatan yang berlawanan. Normalnya,

[49] Youky Surinda, *Konsep Tanggung Jawab Menurut Teori Tanggung Jawab Dalam Hukum*, diakses melalui: http://id.linkedin.com, diakses pada tanggal 25 Mei 2025.

dalam kasus sanksi dikenakan terhadap pelaku adalah karena perbuatannya sendiri yang membuat orang tersebut harus bertanggung jawab".[50]

Hans Kelsen membagi mengenai tanggung jawab menjadi 4 (empat) yaitu:[51]

1. Pertanggungjawaban individu, yaitu seorang individu bertanggung jawab terhadap pelanggaran yang di lakukan nya sendiri;
2. Pertanggungjawaban kolektif, yaitu seorang individu bertanggung jawab atas suatu pelanggaran yang di lakukan oleh orang lain;
3. Pertanggungjawaban berdasarkan kesalahan, yaitu bahwa seorang individu bertanggung jawab atas pelanggaran yang di lakukannya karena sengaja dan diperkirakan dengan tujuan menimbulkan kerugian; dan
4. Pertanggungjawaban mutlak yaitu, seorang individu bertanggung jawab atas pelanggaran yang di lakukannya karena tidak sengaja dan tidak diperkirakan.

Pertanggungjawaban dalam kamus hukum terdapat dua istilah yakni liability (menunjuk pertanggungjawaban hukum yaitu tanggung gugat akibat kesalahan yang dilakukan oleh subjek hukum) dan *responsibility* (menunjuk pada pertanggungjawaban politik). "Teori tanggung jawab hukum lebih menekankan pada makna tanggung jawab yang lahir dari ketentuan Peraturan Perundang-Undangan sehingga teori tanggung jawab dimaknai dalam arti *liability*".[52] Sedangkan tanggung jawab adalah keadaan dimana seseorang wajib menanggung segala perbuatannya bila terjadi hal yang tidak di inginkan boleh dituntut, dipersalahkan atau diperkarakan.

Secara umum pertanggungjawaban hukum dapat dibagi menjadi 2 (dua) bentuk yaitu : 1) Pertanggungjawaban Hukum Perdata; dan 2) Pertanggungjawaban Hukum Pidana

---

[50] Ridwan HR, *Hukum Administrasi Negara*, Rajawali Pers, Jakarta, 2016, h. 318.

[51] Hans Kelsen, *Teori Hukum Murni, terjemahan Rasul Mutaqien*, Nuansa & Nusa Media, Bandung, 2006, h. 140.

[52] Azheri, *Corporate Social Responbility: Dari Voluntary Menjadi Mandatory*, PT Raja Grafindo Persada, Jakarta, 2011, h. 54.

1) Pertanggungjawaban Hukum Perdata

Pertanggungjawaban hukum perdata dapat berupa pertanggungjawaban hukum berdasarkan wanprestasi dan perbuatan melawan hukum (*onrechtmatige daad*). Pertanggungjawaban hukum perdata berdasarkan wanprestasi baru dapat ditegakkan dengan terlebih dahulu harus adanya perjanjian yang melahirkan hak dan kewajiban. Perjanjian diawali dengan adanya persetujuan para pihak. Berdasarkan Pasal 1313 Kitab Undang-Undang Hukum Perdata definisi persetujuan adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih. "Dalam hubungan hukum para pihak yang berlandaskan perikatan, pihak yang dibebankan suatu kewajiban, kemudian tidak melaksanakan atau melanggar kewajiban yang dibebankan kepadanya maka dapat dinyatakan lalai dan atas dasar kelalaian itu maka dapat dituntut pertanggungjawaban hukum perdata berdasarkan wanprestasi".[53] "Dari ketentuan Pasal 1234 KUHPerdata yang berbunyi "Perikatan ditujukan untuk memberikan sesuatu, untuk berbuat sesuatu, atau untuk tidak berbuat sesuatu".[54]

Sedangkan pertanggungjawaban hukum perdata berdasarkan perbuatan melawan hukum (*onrechtmatige daad*) didasarkan pada adanya hubungan hukum, hak dan kewajiban. Konsepsi perbuatan melawan hukum di Indonesia didasarkan pada Pasal 1365 KUHPerdata yang berbunyi: Tiap perbuatan yang melanggar

---

[53] Ade Sanjaya, *Pengertian Prestasi Wanprestasi Definisi Dalam Hukum Perdata Menurut Para Ahli dan Macam Macamnya,* diakses melalui: http://www.landasanteori.com/2015/09/pengertian-prestasi-wanprestasi.html, 25 Mei 2025.

[54] Bung Pokrol, *Perbuatan Melanggar Hukum Dan Wanprestasi,* diakses melalui: http://www.hukumonline.com/klinik/detail/c/2008/perbuatan-melanggar-hukum-atau wanprestasi, diakse pada tanggal 25 Mei 2025.

hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut.

Suatu perbuatan dikatakan merupakan suatu perbuatan melawan hukum dan dapat dimintakan pertanggungjawaban untuk membayar ganti rugi apabila memenuhi unsur-unsur sebagai berikut, yaitu:[55]

1. Unsur Perbuatan. Unsur perbuatan sebagai unsur yang pertama dapat digolongkan dalam dua bagian yaitu perbuatan yang merupakan kesengajaan (dilakukan secara aktif) dan perbuatan yang merupakan kelalaian (pasif/tidak berniat melakukannya);
2. Melawan hukum. Perbuatan melawan hukum diartikan tidak hanya perbuatan yang melanggar kaidah-kaidah tertulis, yaitu perbuatan yang bertentangan dengan kewajiban hukum si pelaku dan melanggar kaidah hak subyektif orang lain, tetapi juga perbuatan yang melanggar kaidah yang tidak tertulis, yaitu kaidah yang mengatur tata susila, kepatutan, ketelitian dan kehati-hatian yang seharusnya dimiliki seseorang dalam pergaulan hidup dalam masyarakat atau terhadap harta benda warga masyarakat;
3. Adanya kerugian. Pasal 1365 KUHPerdata menentukan kewajiban pelaku perbuatan melawan hukum untuk membayar ganti rugi. Namun tidak ada pengaturan lebih lanjut mengenai ganti kerugian tersebut. Pasal 1371 ayat (2) KUHPerdata memberikan sedikit pedoman untuk itu dengan menyebutkan penggantian kerugian dinilai menurut kedudukan dan kemampuan kedua belah pihak dan menurut keadaan. Selanjutnya dapat ditemukan pedoman pada Pasal 1372 ayat (2) KUHPerdata yang menyatakan dalam menilai satu dan lain, hakim harus memperhatikan berat ringannya penghinaan, begitu pula pangkat, kedudukan dan kemampuan kedua belah pihak, dan pada keadaan; dan
4. Adanya hubungan kausalitas antara kesalahan dan kerugian. Dalam perbuatan melawan hukum adalah unsur kausalitas sangat penting, dimana harus dapat dibuktikan bahwa kesalahan dari seseorang menyebabkan kerugian kepada orang lain atau kerugian dari orang lain benar-benar disebabkan oleh kesalahan orang yang digugat. Sehingga kesalahan dan kerugian memiliki hubungan yang erat dan merupakan satu kesatuan yang tidak dapat dipisahkan.

---

[55] Kiki Nitalia Hasibuan, *Masalah Pertanggung Jawab Hukum Dalam Kasus Mis Selling*, diakses melalui: http://lontar.ui.ac.id/file?file=digital/13bogo-T+28032-MisSelling+dalam-metodologi.pdf, diakses pada tanggal 25 Mei 2025.

Pertanggungjawaban hukum perdata dengan dasar perbuatan melawan hukum dan wanprestasi adalah ganti rugi. Namun terdapat perbedaan di antara keduanya, yaitu tujuan atau akibat akhir dari perbuatan melawan hukum adalah ganti rugi sebagai upaya pemulihan sebagaimana keadaan semula sebelum terjadinya perbuatan melawan hukum tersebut. Sedangkan tujuan atau akibat akhir dari ganti rugi dalam wanprestasi adalah ganti rugi merupakan pelaksanaan kewajiban dari pihak debitur. Dapat pula diartikan bahwa ganti rugi dalam wanprestasi dimaksudkan agar para pihak melakukan pembayaran tepat pada waktunya.

Selain itu berdasarkan ketentuan Pasal 1365 KUHPerdata yang berbunyi tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut, sehingga dapat dimaknai kerugian akibat perbuatan melawan hukum sebagai rugi (*scade*) saja. "Kerugian akibat wanprestasi berdasarkan ketentuan Pasal 1246 KUHPerdata yang berbunyi biaya, ganti rugi dan bunga, yang boleh dituntut kreditur, terdiri atas kerugian yang telah dideritanya dan keuntungan yang sedianya dapat diperolehnya, tanpa mengurangi pengecualian dan perubahan yang disebut di bawah ini, dapat disimpulkan berupa biaya, kerugian dan bunga".[56]

Tanggung jawab dalam arti hukum, ialah tangung jawab yang benar benar terkait dengan hak dan kewajiban. Pelaku usaha dalam menjalankan usahanya memiliki tanggung jawab terhadap konsumen atas segala tindakan yang dapat

---

[56] M. Yahya Harahap, *Hukum Acara Perdata*, Sinar Grafika, Jakarta, 2013, h. 448.

merugikan konsumen termasuk kerugian yang diderita oleh seorang pemakai produk yang cacat atau membahayakan, bahan juga pemakai yang turut menjadi korban, merupakan tanggung jawab pelaku usaha. Dari uraian tesebut, maka prinsip tanggung jawab merupakan perihal yang sangat penting dalam hukum perlindungan konsumen. "Membahas mengenai pertanggungjawaban maka tidak lepas dari adanya prinsip-prinsip mengenai tanggung jawab, karena prinsip tanggung jawab merupakan hal yang sangat penting dalam perlindungan konsumen".[57]

2) Pertanggungjawaban Pidana

Pertanggungjawaban hukum pidana adalah suatu kewajiban untuk membayar pembalasan yang akan di terima pelaku dari seseorang yang telah di rugikan, dan juga bahwa pertanggungjawaban yang dilakukan tersebut tidak hanya menyangkut masalah hukum semata akan tetapi menyangkut pula masalah nilai-nilai moral ataupun kesusilaan yang ada dalam suatu masyarakat. "Pertanggungjawaban hukum pidana dalam bahasa asing disebut sebagai *toereken-baarheid*, *criminal reponsibilty*, *criminal liability*, pertanggungjawaban pidana disini dimaksudkan untuk menentukan apakah seseorang tersebut dapat dipertanggung jawabkan secara pidana atau tidak terhadap tindakan yang dilakukannya itu".[58]

Terkait pertanggungjawaban hukum pidana terdapat sebuah prinsip yang sangat penting dari Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana yang

---

[57] Shidarta, *Hukum Perlindungan Konsumen Indonesia*, PT Grasindo, Jakarta, 2000, h. 58.

[58] Daud Hidayat Lubis, *Pertanggung Jawaban Pidana Anak Menurut Hukum Pidana Positif Dan Hukum Pidana Islam*, diakses melalui: http://repository.usu.ac.id/bitstream/123456789/25809/3/Chapter%2011.pdf, diakses pada tanggal 25 Mei 2025.

menyatakan “suatu perbuatan hanya merupakan tindak pidana, jika ini ditentukan lebih dulu dalam suatu ketentuan perundang-undangan”. Oleh karena itu, seseorang hanya bisa dituntut untuk melaksanakan pertanggungjawaban hukum pidana, apabila perbuatan orang tersebut merupakan suatu tindakan pidana yang telah diatur oleh hukum dan dapat dikenai hukuman pidana. “Tindakan pidana tersebut harus ada suatu akibat tertentu dari perbuatan pelaku berupa kerugian atas kepentingan orang lain, menandakan keharusan ada hubungan sebab akibat antara perbuatan pelaku dan kerugian atas kepentingan tertentu”.[59]

3.2. Pertanggungjawaban Pelaku *Cyber Espionage* Berdasarkan Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Pidana Indonesia tidak secara eksplisit menyebutkan *cyber espionage* karena disusun jauh sebelum munculnya teknologi digital. Namun, beberapa Pasal dalam Kitab Undang-Undang Hukum Pidana dan peraturan perundang-undangan lain dapat dikenakan terhadap pelaku spionase siber, terutama jika tindakannya menimbulkan kerugian bagi negara. Walaupun Kitab Undang-Undang Hukum Pidana belum spesifik, pelaku *cyber espionage* bisa dijerat melalui Pasal-Pasal analogi berikut.

Mengenai tindak pidana terhadap Keamanan Negara maka pelaku tindak pidana *cyber espionase* dapat dijerat dengan Pasal 112 dan Pasal 113 Kitab Undang-Undang Hukum Pidana.

Pasal 112

> Barang siapa dengan sengaja mengumumkan surat-surat, berita-berita atau keterangan keterangan yang diketahuinya bahwa harus dirahasiakan untuk

---

[59] Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana Indonesia*, Refika Aditama, Bandung, 2009, h. 59.

kepentingan negara, atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun.

Pasal 113

1) Barang siapa dengan sengaja, untuk seluruhnya atau sebagian mengumumkan, atau memberitahukan maupun menyerahkan kepada orang yang tidak berwenang mengetahui, surat-surat, peta-peta, rencana-rencana, gambar-gambar atau benda-benda yang bersifat rahasia yang bersangkutan dengan pertahanan atau keamanan Indonesia terhadap serangan dari luar, yang ada padanya atau yang isinya, bentuknya atau susunanya benda- benda itu diketahui olehnya, diancam dengan pidana penjara paling lama empat tahun.
2) Jika surat-surat atau benda-benda ada pada yang bersalah, atau pengetahuannya tentang itu karena pencariannya, pidananya dapat ditambah sepertiga

Jika pencurian tersebut merupakan suatu hal yang bersifat rahasia, maka pelaku *cyber espionage* dapat dijerat dengan Pasal 322 ayat (1) yang berbunyi: Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah. Dan ayat (2) yang berbunyi: Jika kejahatan dilakukan terhadap seorang tertentu, maka perbuatan itu hanya dapat dituntut atas pengaduan orang itu.

Sedangkan mengenai Pencurian Informasi yang dilakukan oleh pelaku *cyber espionage* maka dalam Kitab Undang-Undang Hukum Pidana dapat dikenakan Pasal 362 KUHP.

Pasal 362

Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan

hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah.

Pertanggungjawaban pelaku *cyber espionage* berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia dapat dikenakan melalui beberapa ketentuan hukum pidana umum, meskipun secara spesifik istilah *cyber espionage* belum diatur secara eksplisit dalam KUHP. Tindakan *cyber espionage*, yang mencakup peretasan sistem elektronik untuk memperoleh informasi rahasia, dapat dikenai pertanggungjawaban pidana berdasarkan Pasal 30 dan Pasal 31 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Namun, jika dikaitkan dengan Kitab Undang-Undang Hukum Pidana, perbuatan ini dapat dikualifikasikan sebagai bentuk tindak pidana pencurian data (analog dengan Pasal 362 KUHP tentang pencurian) atau pelanggaran terhadap rahasia negara (misalnya Pasal 112 dan Pasal 113 KUHP). Dalam hal pelaku terbukti memiliki niat jahat (*mens rea*) dan melakukan tindakan yang merugikan negara atau individu secara melawan hukum (*actus reus*), maka ia dapat dimintai pertanggungjawaban pidana sesuai prinsip umum dalam hukum pidana Indonesia. Perlu adanya harmonisasi antara Kitab Undang-Undang Hukum Pidana dan regulasi khusus seperti Undang-Undang Informasi dan Transaksi Elektronik agar penegakan hukum terhadap pelaku *cyber espionage* dapat berjalan lebih efektif dan komprehensif.

3.3. Pertanggungjawaban Pelaku *Cyber Espionage* Diluar Kitab Undang-Undang Hukum Pidana

Pertanggungjawaban pelaku *cyber espionage* (mata-mata siber) di luar Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia dapat dianalisis melalui berbagai undang-undang sektoral dan prinsip hukum internasional. Meskipun KUHP Indonesia belum secara eksplisit mengatur *cyber espionage*, terdapat beberapa regulasi lain yang dapat dijadikan dasar pertanggungjawaban.

Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan perubahannya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Maka pelaku *cyber espionage* dapat dijerat dengan Pasal 30 mengenai akses ilegal sistem elektronik, Pasal 31 mengenai penyadapan atas informasi elektronik atau dokumen elektronik., Pasal 32 mengenai perubahan, penghapusan, atau pengrusakan informasi elektronik, dan Pasal 35 mengenai pemalsuan informasi elektronik.

Pasal 30

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan Undang-Undang.
4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Adapun saksi dan hukuman bagi pelaku *cyber espionage* jika melanggar Pasal 30, Pasal 31, Pasal 32 dan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik tersebut, maka pelaku dapat dikenakan saksi sebagaimana Pasal 46, Pasal 47, Pasal 48 dan Pasal 51 Undang-Undang Nomor 19 Tahun 2016

tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 46

1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).
2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 48

1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah).
2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp.3.000.000.000,00 (tiga miliar rupiah).
3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.5.000.000.000,00 (lima miliar rupiah).

Pasal 51

1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah).
2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah).

Sedangkan dalam Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memuat larangan bagi pihak-pihak yang melakukan spionase terhadap negara, sebagaimana Pasal 44 menyatakan bahwa setiap orang yang

membocorkan rahasia intelijen negara dapat dikenakan sanksi pidana. Dan dalam Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara dalam konteks pertahanan, *cyber espionage* terhadap data strategis negara dapat dikategorikan sebagai bentuk ancaman non-militer, dan pelakunya dapat dikenai sanksi berdasarkan Undang-Undang lain yang relevan.

Sehingga mengenai pertanggungjawaban pelaku *cyber espionage* di luar Kitab UndangUndang Hukum Pidana dan pentingnya pengembangan kerangka hukum nasional yang responsif terhadap ancaman siber. Saat ini, hukum positif Indonesia belum secara eksplisit mengatur tindak pidana *cyber espionage*, sehingga menimbulkan kekosongan norma (*normative gap*) dan hambatan dalam penegakan hukum. Dalam konteks ini, pelaku cyber espionage sulit dipertanggungjawabkan secara pidana jika hanya merujuk pada Kitab Undang-Undang Hukum Pidana, karena delik yang dilakukan bersifat lintas batas dan berbasis teknologi tinggi. Oleh karena itu, diperlukan regulasi khusus di luar Kitab Undang-Undang Hukum Pidana, seperti penguatan Undang-Undang Informasi dan Transaksi Elektronik, pembentukan Undang-Undang khusus kejahatan siber, serta harmonisasi dengan instrumen hukum internasional. Isu hukum normatif yang muncul, seperti asas legalitas, kejelasan norma, dan yurisdiksi, juga harus menjadi perhatian agar pertanggungjawaban pelaku *cyber espionage* dapat ditegakkan secara adil dan efektif sesuai prinsip negara hukum.

3.4. Pertanggungjawaban Pelaku *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia

Cyber espionage yang dapat disebut sebagai "*cyber-exploitation*" juga didefinisikan oleh "Herbert Lin sebagai tindakan dan operasi dalam jangka waktu yang lama untuk memperoleh informasi yang seharusnya dijaga kerahasiaannya dan berada di transit melalui sistem komputer atau jaringan negara musuh".[60] Sebelum memasuki penjelasan bagaimana hukum internasional mengatur *cyber espionage* terhadap negara-negara, ada beberapa terminologi seperti *cyber space*, *cyber crime* dan *cyber law* yang akan membantu untuk memahami bagaimana dan dimana *cyber espionage* dilakukan. Paling pertama adalah *cyber space*,

Definisi terbaru dari *cyber space* oleh "FD Kramer adalah domain global dan dinamis (dapat berubah terus menerus) yang dicirikan oleh penggunaan gabungan elektron dan spektrum elektromagnetik, yang bertujuan untuk membuat, menyimpan, memodifikasi, bertukar, berbagi, dan mengekstrak, menggunakan, menghilangkan informasi, dan mengganggu sumber daya fisik".[61]

> Barda Nawawi[11] merujuk kepada kerangka sistematik dari *Draft Convention* on *cybercrime* dari Dewan Eropa (Draft No.25, Desember 2000) yang sekarang telah berubah menjadi Budapest Convention mendefinisikannya secara sederhana sebagai "*crime related to technology, computers, and the internet*" atau secara sederhana sebagai kejahatan yang berhubungan dengan teknologi, komputer dan internet.[62]

---

[60]Aldo Rahmandana, *Tinjauan Yuridis Cyber Espionage Berdasarkan Hukum Internasional*, Jurnal Jurist-Diction, Vol.4, No.6, 2021, h. 2144.

[61] *Ibid*.

[62] Masitoh Indriani, *Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cyber Crime Dalam Sistem Transaksi Elektronik*, Jurnal Yuridika, Vol.29, No.3, 2014, h. 333.

"*Cyber law* merupakan hukum yang digunakan di dunia *cyber* yang umumnya dikorelasikan dengan *internet*".[63] Ruang lingkup yang terkandung dalam *cyber law* adalah segala aspek yang berhubungan dengan subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat "*online*" dan memasuki dunia *cyber* atau maya.

Meskipun istilah "*cyber espionage*" belum secara eksplisit disebutkan dalam peraturan perundang-undangan Indonesia, beberapa instrumen hukum berikut dapat digunakan untuk menjerat pelaku. Diantaranya dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dalam Pasal 30 yang dinyatakan bahwa: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain".

Sedangkan dalam Pasal 31 Undang-Undang Informasi dan Transaksi Elektronik melarang intersepsi terhadap transmisi informasi elektronik atau dokumen elektronik tanpa hak. Begitu juga dalam Pasal 32 dan Pasal 33 melarang perusakan, pengubahan, penghilangan informasi elektronik atau dokumen elektronik. Adapun sanksi pidana diatur dalam Pasal 46 dan Pasal 47 Undang-Undang Informasi dan Transaksi Elektronik, dengan hukuman penjara hingga 8 tahun dan/atau denda maksimal Rp.800.000.000.00 (delapan ratus juta rupiah)

Dalam Kitab Undang-Undang Hukum Pidana sendiri pelaku cyber espionage mestinya dapat dijerat dengan Pasal 112 dan Pasal 113 KUHP (tentang

---

[63]Asril Sitompul, *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace,* Citra Aditya Bakti, Bandung, 2001, h. 56.

spionase. Berlaku untuk spionase konvensional, bisa diperluas interpretasinya untuk mencakup aktivitas siber dengan pendekatan analogi hukum.

Maka berdasarkan penjelasan-penjelasan diatas penulis menarik kesimpulan bahwa *cyber espionage* atau spionase siber merupakan tindakan pencurian data atau informasi penting melalui jaringan komputer, yang umumnya dilakukan untuk kepentingan politik, ekonomi, atau militer suatu negara atau kelompok tertentu. Dalam konteks hukum positif Indonesia, tindakan ini dapat dikategorikan sebagai tindak pidana, meskipun belum ada aturan yang secara eksplisit menyebut istilah "*cyber espionage*". Namun, beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, dapat dijadikan dasar pertanggungjawaban pelaku. Pasal-Pasal yang mengatur tentang akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), dan manipulasi data atau sistem elektronik (Pasal 32 dan Pasal 33) dapat digunakan untuk menjerat pelaku *cyber espionage*. Selain itu, jika tindakan tersebut mengancam keamanan negara atau membahayakan kepentingan nasional, pelaku juga dapat dijerat dengan Pasal-Pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) tentang kejahatan terhadap keamanan negara. Oleh karena itu, meskipun adanya kekosongan hukum terkait regulasi yang khusus mengenai *cyber espionage*, pelaku tetap dapat dimintai pertanggungjawaban pidana berdasarkan ketentuan yang ada dalam hukum positif Indonesia.

BAB IV

PENUTUP

4.1. Kesimpulan

1. Mengenai pengaturan tindak pidana *cyber espionage* dalam hukum positif di Indonesia bahwa hukum positif yang ada menunjukkan adanya kekosongan normatif dan belum adanya regulasi khusus yang secara tegas dan terperinci mengatur *cyber espionage* sebagai tindak pidana tersendiri. Untuk menjamin kepastian hukum dan efektivitas penegakan hukum terhadap kejahatan ini.
2. Meskipun belum ada aturan yang secara eksplisit menyebut istilah "*cyber espionage*". Namun, beberapa ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dapat dijadikan dasar pertanggungjawaban pelaku. Pasal-Pasal yang mengatur tentang akses *ilegal* (Pasal 30), intersepsi *ilegal* (Pasal 31), dan manipulasi data atau sistem elektronik (Pasal 32 dan Pasal 33) dapat digunakan untuk menjerat pelaku *cyber espionage*. Selain itu, jika tindakan tersebut mengancam keamanan negara atau membahayakan kepentingan nasional, pelaku juga dapat dijerat dengan Pasal-Pasal KUHP tentang kejahatan terhadap keamanan negara.

4.2. Saran

1. Pemerintah diharapkan melakukan pembaruan dan harmonisasi peraturan perundang-undangan yang relevan, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), agar secara eksplisit mencakup tindak pidana spionase siber.

2. Pemerintah perlu membentuk satuan tugas khusus di bawah lembaga penegak hukum yang memiliki kompetensi teknis di bidang keamanan siber guna mempercepat proses identifikasi, investigasi, dan penindakan pelaku. Kerja sama internasional juga harus diperkuat, mengingat *cyber espionage* sering melibatkan aktor lintas negara.

DAFTAR BACAAN

Buku-Buku

Azheri, *Corporate Social Responbility: Dari Voluntary Menjadi Mandatory*, PT Raja Grafindo Persada, Jakarta, 2011.

H.M., Jogiyanto, *Pengenalan Komputer*, Cetakan Pertama, Andi Ofset, Jogyakarta, 2005.

Herrmann, Dominik, *Cyber Espionage and Cyber Defence*, *Information Technology for Peace and Security,* Springer Vieweg, Wiesbaden, 2019.

Harahap, M. Yahya, *Hukum Acara Perdata*, Sinar Grafika, Jakarta, 2013.

HR, Ridwan, *Hukum Administrasi Negara*, Rajawali Pers, Jakarta, 2016.

Hollis, Duncan B., *A Brief Primer on International Law and Cyberspace*, Carnegie Endowment for International Peace, 2021.

International Groups of Experts at the Invitation of the NATO CCDCOE, *Tallinn Manual 2.0*, Cambridge University Press, Cambridge, 2017.

Kelsen, Hans, *Teori Hukum Murni, terjemahan Rasul Mutaqien*, Nuansa & Nusa Media, Bandung, 2006.

Makarim, Edmon, *Kompilasi Hukum Telematika*, Cet.2, PT Raja Grafindo Persada, Jakarta, 2004.

Moeljatno, *Asas-Asas Hukum Pidana*, Cet.VII, Rineka Cipta, Jakarta, 2002.

Maskun dan Wiwik Meilarati, *Aspek Hukum Penipuan Berbasis Internet*, Keni Media, Bandung, 2017.

Prodjodikoro, Wirjono, *Asas-Asas Hukum Pidana Indonesia*, Refika Aditama, Bandung, 2009.

Raharjo, Satjipto, *Ilmu Hukum*, PT Citra Aditya Bakti, Bandung, 2000.

Raharjo, Agus, *Cybercrime*, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Citra Aditya Bakti, Bandung, 2002.

Rubenstein, Dana, *Nation State Spionase Cyber and its Impacts,* Paper Washington University, St. Louis, 2014.

Shidarta, *Hukum Perlindungan Konsumen Indonesia*, PT Grasindo, Jakarta, 2000.

Sutarman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, Laks Bang PRESSindo, Jogjakarta, 2007.

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

Sitompul, Asril, *Hukum Internet (Pengenalan Mengenai Masalah Hukum di Cyberspace,* Citra Aditya Bakti, Bandung, 2001.

Suyanto, *Penelitian Hukum Pengantar Penelitian Normatif Empiris dan Gabungan*, Cetakan Pertama, Unigres Press, Gresik, 2022.

Tim Dosen Fakultas Hukum Universitas Brawijaya, *Ketika Hukum Berhadapan Dengan Globalisasi*, UB Press, Malang, 2011.

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

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

Wijayanti, Asri, *Strategi Penulisan Hukum*, Lubuk Agung, Bandung, 2011.

Skripsi-Skripsi

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

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

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

Makalah-Makalah

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

Jurnal-Jurnal

E. Gindin, Susan, *Lost and Found in Cyberspace: Informational Privacy in The Age of The Internet*, Jurnal San Diego Law Review 1153, 1997.

Indriani, Masitoh, *Implementasi Peraturan Pemerintah Nomor 82 Tahun 2012 Sebagai Upaya Negara Mencegah Cyber Crime Dalam Sistem Transaksi Elektronik*, Jurnal Yuridika, Vol.29, No.3, 2014.

Rahmandana, Aldo, *Tinjauan Yuridis Cyber Espionage Berdasarkan Hukum Internasional*, Jurnal Jurist-Diction, Vol.4, No.6, 2021.

Media Daring

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.

Boytra, *Cerita Sedikit Tentang Spyware*, diakses melalui: www.boytra.blogspot.com/2007/08/cerita-sedikit-tentang-spyware.html, diakse pada tanggal 1 Mei 2025.

Cambridge Dictionary, *Espionage,* diakses melalui: https://dictionary.cambridge.org/dictionary/english/espionage, diakses pada tanggal 04 Desember 2024.

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

Hasibuan, Kiki Nitalia, *Masalah Pertanggung Jawab Hukum Dalam Kasus Mis Selling*, diakses melalui: http://lontar.ui.ac.id/file?file=digital/13bogo-T+28032-MisSelling+dalam-metodologi.pdf, diakses pada tanggal 25 Mei 2025.

ICRC (*International Committee of the Red Cross*), *Cyber Warfare and International Humanitarian Law: The ICRC's Position*, diakses melalui: https://www.icrc.org/en/doc/assets/files /2013/130621-cyberwarfare-q-and-a-eng.pdf, diakses pada tanggal 1 Mei 2025.

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.

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.

Majelis Eropa, *The Budapest Convention on Cyber Crime: Benefits and Impact in Practice Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-repprovisional/16809ef6c, diakse pada tanggal 1 Mei 2025.

Majelis Eropa, ***C****ybercrime Investigation and The Protection of Personal Data and Privacy Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-repprovisional/16809ef6a, diakses pada tanggal 1 Mei 2025.

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.

Surinda, Youky, *Konsep Tanggung Jawab Menurut Teori Tanggung Jawab Dalam Hukum*, diakses melalui: http://id.linkedin.com, diakses pada tanggal 25 Mei 2025.

Wikipedia, *Sejarah Espionase*, diakses melalui: www.wikipedia/spionase/sejarah.com, diakses pada tangal 1 Mei 2025.

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.

Wikipedia, *Spionase*, diakses melalui: www.Wikipedia/spionase.com, diakses pada tanggal 1 Mei 2025.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Undang-Undang Nomor 13 Tahun 2016 tentang Perlindungan Saksi dan Korban.

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 (KUHP Baru)

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

BAB LENGKAP-6.doc

ORIGINALITY REPORT

29%	29%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.unair.ac.id Internet Source	15%
2	elibs.unigres.ac.id Internet Source	8%
3	123dok.com Internet Source	6%

Exclude quotes	Off	Exclude matches	< 6%
Exclude bibliography	Off		