Jurnal Duta Hukum:
Jurnal Penelitian Bidang Hukum Universitas Gresik
Volume xx Nomor xx, Desember 2022
pISSN xxxx-xxxx - eISSN xxxx-xxxx

PERTANGGUNGJAWABAN TINDAK PIDANA *CYBER ESPIONAGE* DI INDONESIA

Muhammad Fadhil Danuarta
Fakultas Hukum Universitas Gresik
Jl. Arif Rahman Hakim 61111, Gresik, Indonesia
Telp. 088989197089
E-mail : fh.unigres@gmail.com

Tulisan Diterima: xx-xx-2025; Direvisi: xx-xx-2025; Disetujui Diterbitkan: xx-xx-2025
DOI:http://dx.doi.org/xxxxx/prohukum.2025.V15.xxx-xxx

Abstrak

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. Penulis mengangkat dua permasalahan. yaitu: 1) Bagaimana pengaturan tindak pidana *cyber espionage* dalam hukum positif di Indonesia; dan 2) Bagaimana pertanggungjawaban pelaku tindak pidana *cyber espionage* berdasarkan hukum positif di Indonesia. Metode penelitian hukum normatif dengan tiga metode pendekatan antara lain pendekatan konseptual, pendekatan perundang-undangan, dan pendekatan historis. Hasil penelitian bahwa 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. Dan 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

Kata Kunci: Pertanggungjawaban; Tindak Pidana; *Cyber Espionage*.

PENDAHULUAN

Latar Belakang

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 menemukan informasi rahasia, khususnya informasi militer atau politik dari negara lain atau informasi industrial dari suatu bisnis".[1] 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".[2]

Hukum internasional telah mengatur tentang spionase dalam masa perang. "Salah satu kodifikasi awal terkait spionase dalam masa perang di era

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

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

modern dapat dilihat dalam Deklarasi Brussels 1874. Deklarasi ini tidak diadopsi oleh para pihak",[3] 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 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".[4] 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 untuk diselesaikan karena identitas penyerang tidak mudah untuk diketahui secara pasti".[5]

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 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.

[3] 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.

[4] 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.

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

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.

Rumusan Masalah

Dari rangkaian latar belakang masalah yang telah diuraikan 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 ?

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.

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. Metode penelitian ini terdiri dari:

1. Jenis Penelitian : Jenis penelitian ini adalah penelitian hukum normatif, penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum. 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.
2. 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. Adapun dalam penelitian ini penulis menggunakan tiga metode pendekatan antara lain pendekatan konseptual (*conceptual approach*), pendekatan perundang-undangan (*statute approach*), dan pendekatan historis (*historical approach*).
3. Metode Pengumpulan Data : Dalam penelitian hukum normatif, teknik pengumpulan bahan hukum dengan cara 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).
4. Teknik Analisa Data : 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.

PEMBAHASAN

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".[6] Sejarah mengenai spionase ini sendiri pun terdokumentasi dengan baik dimulai dari sejak jaman-jaman kekaisaran hingga jaman modern sekarang ini di berbagai belahan

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

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 mengenai informasi tersebut dan akan membocorkannya melalui berbagai dalih".[7]

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.*[8]

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.

Modus Operandi *Cyber Espionage*

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 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*."[9] 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.

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

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

[7] *Ibid.*

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

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

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 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.[10]

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".[11] 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.

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

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.

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.

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

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

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.

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

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".

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)".

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.[12]

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 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*.

Pertanggungjawaban Hukum

"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".[13] 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, dalam kasus sanksi dikenakan terhadap pelaku adalah karena perbuatannya sendiri yang membuat orang tersebut harus bertanggung jawab".[14]

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

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

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

Hans Kelsen membagi mengenai tanggung jawab menjadi 4 (empat) yaitu:[15]

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*".[16] 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

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 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

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

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

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.

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.

Pertanggungjawaban Pelaku *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia

"*Cyber law* merupakan hukum yang digunakan di dunia *cyber* yang umumnya dikorelasikan dengan *internet*".[17] 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

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

dengan Pasal 112 dan Pasal 113 KUHP (tentang 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.

PENUTUP

Kesimpulan

Disimpulkan bahwa 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.

Sedangkan 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.

Saran

Adapun sebagai bentuk saran dalam penelitian ini yakni:

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.

UCAPAN TERIMA KASIH

Dengan terselesaikannya penelitian ini, penulis mengucapkan terima kasih kepada bapak dan ibu guru yang telah membimbing penuh kesabaran dan ketabahan, tak lupa juga kepada orang tua tercinta, ibu dan ayah, yang memberikan kasih sayang dan doa tak henti-hentinya untuk selalu mendukung kemajuan anak-anaknya, dan semoga Allah SWT selalu memberikan kasih sayang kepada mereka di dunia dan akhirat. Serta kepada teman-teman Fakultas Hukum Universitas Gresik angkatan 2021 atas kebersamaannya selama menempuh pendidikan dan berbagi pengetahuan. Semua pihak yang tidak dapat disebutkan satu persatu. Semoga segala bantuan yang diberikan kepada penulis mendapatkan pahala oleh Tuhan Yang Maha Esa. Akhir kata penulis menyadari bahwa skripsi ini masih belum sempurna namun besar harapan penulis semoga tulisan ini dapat berguna dan bermanfaat untuk kita semua, terlebih untuk pihak-pihak yang membutuhkan sebagai bahan rujukan atau referensi dikemudian hari. Aamiin.

DAFTAR PUSTAKA

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

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 (Online)*, diakses melalui: https://dictionary.cambridge.org/dictionary/ english/espionage, diakses pada tanggal 04 Desember 2024.

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

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

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

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

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.

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

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

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

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

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

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

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