

## **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”.<sup>49</sup> 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,

---

<sup>49</sup> 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”.<sup>50</sup>

Hans Kelsen membagi mengenai tanggung jawab menjadi 4 (empat) yaitu:<sup>51</sup>

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*”.<sup>52</sup> 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

---

<sup>50</sup> Ridwan HR, *Hukum Administrasi Negara*, Rajawali Pers, Jakarta, 2016, h. 318.

<sup>51</sup> Hans Kelsen, *Teori Hukum Murni, terjemahan Rasul Mutaqien*, Nuansa & Nusa Media, Bandung, 2006, h. 140.

<sup>52</sup> Azheri, *Corporate Social Responsibility: 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”.<sup>53</sup> “Dari ketentuan Pasal 1234 KUHPerdata yang berbunyi “Perikatan ditujukan untuk memberikan sesuatu, untuk berbuat sesuatu, atau untuk tidak berbuat sesuatu”.<sup>54</sup>

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

---

<sup>53</sup> 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.

<sup>54</sup> Bung Pokrol, *Perbuatan Melanggar Hukum Dan Wanprestasi*, diakses melalui: <http://www.hukumonline.com/klinik/detail/c/2008/perbuatan-melanggar-hukum-atau-wanprestasi>, diakses 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:<sup>55</sup>

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 KUHPerdara menentukan kewajiban pelaku perbuatan melawan hukum untuk membayar ganti rugi. Namun tidak ada pengaturan lebih lanjut mengenai ganti kerugian tersebut. Pasal 1371 ayat (2) KUHPerdara 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) KUHPerdara 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.

---

<sup>55</sup> 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 KUHPerdota 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 KUHPerdota 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”.<sup>56</sup>

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

---

<sup>56</sup> 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 tersebut, 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”.<sup>57</sup>

## 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 reponsibility*, *criminal liability*, pertanggungjawaban pidana disini dimaksudkan untuk menentukan apakah seseorang tersebut dapat dipertanggung jawabkan secara pidana atau tidak terhadap tindakan yang dilakukannya itu”.<sup>58</sup>

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

---

<sup>57</sup> Shidarta, *Hukum Perlindungan Konsumen Indonesia*, PT Grasindo, Jakarta, 2000, h. 58.

<sup>58</sup> 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”.<sup>59</sup>

### **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 espionage* 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

---

<sup>59</sup> 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 Undang-Undang 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”.<sup>60</sup> 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”.<sup>61</sup>

Barda Nawawini<sup>11</sup> merujuk kepada kerangka sistematis 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.<sup>62</sup>

---

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

<sup>61</sup> *Ibid.*

<sup>62</sup> 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*”.<sup>63</sup> 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

---

<sup>63</sup>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 di atas 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.