http://journal.lldikti9.id/plenojure
Vol 11, No, 2, Oktober 2022, pp 142-158
p-ISSN:2301-7686 dan e-ISSN: 2684-8449
DOI: https://doi.org/10.37541/plenojure.v11i2.818

Implementasi Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Di Bidang Komputer

Muhammad Yunus Idy
Hukum Pidana, Fakultas Hukum, Universitas Islam Makassar, Indonesia
Email Correspondensi: *muhyunusidy.dpk@uim-makassar.ac.id*

Artikel info

Jurnal Ilmu Hukum
LL-DIKTI Wilayah IX Sulawesi

Artikel history:
Received; 06-06-2022
Revised;17-08-2022
Accepted; 19-08-2022

Abstrak. Permasalahan yang dibahas dalam penelitian ini adalah bagaimanakah bentuk upaya penanggulangan *cybercrime* dengan menggunakan sarana penal serta mekanisme pertanggungjawabannya sebagaimana yang diatur dalam undang-undang ITE. Metode penelitian yang digunakan adalah *statuta approach*, *conseptual approach*, dan *comparative approach*. Tipe penelitiannya adalah *Normative Legal Research*. Hasil penelitian menunjukkan bahwa upaya penanggulangan *cybercrime* dengan menggunakan sarana penal atau dengan menggunakan kebijakan/politik hukum pidana (*penal policy*) harus lebih sesuai dengan keadaan atau situasi sekarang dan untuk masa-masa yang akan datang, maka dibentuklah undang-undang ITE untuk mengatasi permasalahan sebelumnya terkait dengan pengaturan tentang penanggulangan *cybercrime* yang masih tersebar diberbagai peraturan perundang-undangan yang berlaku. Pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik dapat dijatuhkan kepada *individu* dan *korporasi*. Namun demikian sistem pertanggungjawaban korporasi belum cukup jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan.

Abstract. *The problem discussed in this study is how the form of cybercrime prevention efforts using penal facilities and accountability mechanisms as stipulated in the ITE law. The research method used is the statute approach, conceptual approach, and comparative approach. The type of research is normative legal research. The results of the study indicate that efforts to overcome cybercrime by using penal facilities or by using criminal law policies/politics (penal policy) must be more in line with the current situation or situation and for the future, so the ITE law was formed to overcome previous problems. Related to the regulation of cybercrime prevention which is still scattered in various applicable laws and regulations. Criminal liability, as stipulated in the law on*

information and electronic transactions, can be imposed on individuals and corporations. However, the corporate responsibility system is not yet clear and detailed, especially with regard to when the corporation is said to have committed a crime, who is responsible, and the criminal sanctions that can be imposed.

Keywords:
Kejahatan; Siber;
Dunia Maya;
Pidana;
Pemidanaan;

PENDAHULUAN

Kejahatan dunia maya atau dikenal juga dengan istilah *cyber crime* adalah suatu istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer, baik sebagai alat, sasaran atau tempat terjadinya kejahatan. Walaupun kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, namun istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana peralatan komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. (Laksana, 2019) Kejahatan ini dapat dilakukan oleh seseorang dari suatu tempat yang sangat pribadi misalnya di kamar tidur, tapi menimbulkan kerugian pada seseorang, atau institusi di tempat lain, yang mungkin terpisahkan oleh jarak ribuan kilometer, bahkan seringkali bersifat lintas batas territorial. Dengan demikian kejahatan ini kemudian membawa sifat *transnational crimes,* yaitu kejahatan yang bersifat lintas batas teritorial (*transnational boundaries*).

Hacking adalah bentuk pertama dalam kejahatan ini (*first crime*) sebagaimana ditetapkan oleh kongres PBB ke-X di Wina tahun 2000. Hal ini disebabkan bentuk perbuatan ini merupakan sesuatu yang istimewa, karena mempunyai kelebihan dari bentuk *cyber crime* lainnya. Diantaranya adalah bahwa pelaku kejahatan ini sudah barang tentu dapat melakukan *cyber crime* lainnya. Secara teknis imbas dari aktivitas *hacking* menghasilkan kualitas akibat yang lebih serius dibandingkan dengan bentuk *cyber crime* lainnya. Untuk menyebarkan gambar porno atau *cyber pornography,* orang tidak perlu kemampuan *hacking,* namun cukup dengan kemampuan minimal di bidang

internet. (Putra, 2014)

Berdasarkan pada berbagai unsur perbuatan yang terdapat dalam Pasal 167 ayat (1) dan (2) Kitab Undang-Undang Hukum Pidana (KUHP) yang berlaku di Indonesia, maka akan timbul pertanyaan jika dikaitkan dengan perbuatan *hacking.* Pertanyaan tersebut adalah; apakah sistem komputer seseorang atau sebuah organisasi, atau *website* dalam jaringan komputer (internet) dapat dikategorikan sebagai objek yang diatur dalam Pasal 167 KUHP. Dengan kata lain, apakah dapat disamakan memasuki sistem komputer orang lain dengan memasuki pekarangan atau rumah orang lain?. Apakah menyadap *password* dapat disamakan dengan menggunakan kunci palsu sebagaimana diatur dalam pasal tersebut? Untuk menjawab pertanyaan tersebut maka hakim harus melakukan penafsiran yang mendalam, yang penggunaanya dalam hukum pidana masih menimbulkan perdebatan.

Model penegakan hukum, yang membutuhkan penafsiran meluas seperti diatas menimbulkan ketidakpuasan dibanyak kalangan. Ketidakpuasan tersebut karena perbedaan persepsi di antara penegak hukum yang menimbulkan diskriminasi dalam penegakan hukum, (Middin et al., 2021) sampai kepada ancaman pidana dalam pasal-pasal KUHP yang tidak sebanding dengan tingkat kerugian yang ditimbulkan oleh *cyber crime.* Desakan kepada pemerintah untuk segera meregulasi bentuk kejahatan ini akhirnya terjawab ketika pemerintah bersama Dewan Perwakilan Rakyat (DPR) menyetujui untuk memberlakukan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Meski tidak secara khusus merupakan undang-undang tentang *cybercrime*, beberapa pasal dalam undang-undang tersebut mengatur tentang *cybercrime.*

Berdasarkan uraian tersebut di atas, maka permasalahan yang hendak dikaji dalam karya tulis ini adalah bagaimanakah bentuk upaya penanggulangan cybercrime atau kejahatan di bidang komputer dengan menggunakan sarana penal serta mekanisme pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik.

Landasan Teori

1. Pengaturan tentang *Cybercrime* secara Internasional

Teknologi mutakhir terus diciptakan untuk dapat membantu segala aktivitas manusia agar lebih mudah, cepat, efektif dan efisien dalam melakukan segala aktifitasnya. Teknologi sebagai karya cipta manusia memiliki sisi positif dan sisi negatif. Namun pada dasarnya, teknologi bersifat netral, artinya dampak positif atau negatif itu muncul tergantung tujuan penggunaannya. Internet adalah merupakan produk teknologi abad ini yang sedang berkembang di dunia, termasuk di Indonesia. (Aswari, 2020)

Berdasarkan definisi yang dikemukakan oleh *The US Supreme Court* bahwa internet disebut sebagai *international Network of interconnected computers, yang* artinya jaringan internasional dari komputer-komputer yang saling berhubungan, (A. Setiawan et al., 2016)sehingga melewati batas-batas territorial suatu Negara. (Wahid, 2005) Melalui internet seseorang dapat melakukan beberapa aktivitas secara bersamaan tanpa harus keluar rumah, misalnya berdiskusi, belanja, transfer uang, kuliah dan lain-lain. Hal ini merupakan sisi positif dari internet, namun internet juga memiliki sisi negatif, karena sering dimanfaatkan sebagai media untuk melakukan kejahatan yang dikenal dengan istilah *cyber crime*. Volodymyr Golubev menyebutnya sebagai *"the new form of anti-social behavior"*. (Golubev, 2012) Ada beberapa jenis kejahatan ini, misalnya *economic cyber crime, cyber terrorism, cyber stalking, cyber sex dan cyberporn.* Hal ini menunjukkan bahwa segala bentuk kejahatan di dunia nyata telah terjadi pula di dunia maya.

Dalam *background paper* lokakarya Kongres PBB X pada tahun 2000 juga memberikan definisi *cybercrime*, akan tetapi membagi definisi tersebut dalam *narrow sense* (*arti sempit*) dan *broader sense* (*arti Luas*), yang menyatakan bahwa:

"Cybercrime in narrow sense is Any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them". "Cybercrime as a broader sense adalah *Any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network".* (Arief, 2006)

Istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*", seringkali digunakan secara bergantian untuk merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. (Wijaya & Arifin, 2020) Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku bisa melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misalnya pencurian atau pemalsuan. (Rahim & Rahim, 2021)

Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global. *Cyber crime* seringkali dilakukan secara transnasional, melintasi batas negara sehingga sulit dipastikan yuridikasi hukum negara yang berlaku terhadap pelaku. Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas *(anonymous)* memungkinkan terjadinya berbagai aktivitas jahat yang tak tersentuh hukum. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain: (Sari, 2019)

1) *Unauthorized Access to Computer System and Service*
2) *Illegal Contents*
3) Data *Forgery*
4) *Cyber Espionage*
5) *Cyber Sabotage and Extortion*
6) *Offense against Intellectual Property*
7) *Infringements of Privacy*

Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai *cybercrime* diatur dalam Pasal 2-5, adapun jenis tindak pidana tersebut adalah :

1) *Illegal Access*

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer. (Keyser, 2017) Perlindungan terhadap pelanggaran *illegal access* ini

merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

2) *Illegal Interception*

Illegal Interception adalah tindakan tidak sah berupa pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

3) *Data Interception*

Data Interception diatur dalam Pasal 4 *Cybercrime Convention,* yang pada dasarnya berkaitan dengan ketentuan pengrusakan data sehingga menjadi tindak pidana. Ketentuan ini bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem komputer. Hal ini merupakan pelangagaran menurut ketentuan dalam pasal ini.

4) *System Interference*

System Interference diatur dalam Pasal 5 *Cybercrime Convention.* Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila *"... when committed intentionally, the serious hindering without right of the functioning of a computer system…"*, yang dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer. Gangguan terhadap sistem dijadikan sebagai tindak pidana dengan bertujuan untuk mencegah *"…the serious hindering without right of the functioning of a computer system..".*

5) *Misuse of Device*

Misuse of Device diatur dalam Pasal 6 konvensi ini adapun yang termasuk jenis kejahatan ini adalah pencurian ,penyediaan, penjualan dan distribusi dari data komputer yang diperoleh dari sebuah alat. Sedangkan yang dimaksud sebagai alat adalah *hardware* maupun *software* yang telah di modifikasi untuk

mendapatkan akses dari sebuah komputer atau jaringan komputer. Contohnya apabila ada sesorang yang memasukkan *keylogger* dalam jaringan bank untuk mendapatkan data-data nasabah mulai dari alamat sampai ke *password* ATM dan data-data tersebut dijual, digunakan atau didistribusikan untuk kejahatan lain.

2. Harmonisasi Konvensi Cybercrime Dalam Hukum Nasional

Indonesia sebagai bagian dari negara bangsa di dunia, termasuk sebagai salah satu negara yang cukup banyak memiliki penyalahgunaan dalam pemanfaatan jaringan internet, khususnya dalam hal pemesanan barang-barang atau perdagangan dengan menggunakan media internet. (Wahyudi, 2006) Kondisi ini dapat merugikan pihak Indonesia, khususnya dalam dunia perdangangan melalui internet, karena transaksi internet dengan menggunakan kartu yang dikeluarkan oleh pihak perbankan Indonesia berpotensi untuk ditolak oleh pihak luar negeri.

European Convention on Cyber Crime merupakan konvensi tentang *cyber crime* yang disepakati oleh Negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi Negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak Negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan cyber crime di berbagai negara. Oleh karenanya menjadi penting bagi Indonesia untuk merujuk konvensi ini sebagai salah satu pembanding dalam pengaturan *cyber crime,* terlebih lagi J.E Sahetapy pernah mengemukakan bahwa hukum pidana di Indonesia, belum siap menghadapi kejatahan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai pencurian. Kalau dikatakan pencurian, tentu harus ada barang yang hilang. Padahal dalam kejahatan komputer, data si pemilik masih ada kendati sudah dicuri orang lain. (WidyoPramono, 1994) Bagaimana dengan *cybercrime*, tentu tantangan yang dihadapi menjadi lebih berat. Barda Nawawi Arief menyatakan bahwa *cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. (Qamar & Aswari, 2018) Ada beberapa faktor yang mempengaruhi terjadinya *cybercrime*, yaitu faktor politik, faktor ekonomi dan faktor sosial budaya. (Sutarwan et al., 2007)

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime* yang dapat menjadi rujukan oleh pihak Indonesia dalam pengaturan tentang *Cyber Crime* adalah :

1) Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system komputer, yaitu:

a) Mengakses system komputer tanpa hak (*illegal acces*);
b) Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
c) Tanpa hak merusak data (*data interference*);
d) Tanpa hak mengganggu system (*system interference*);
e) Menyalahgunakan perlengkapan (*misuse of device*).

2) Delik-delik yang berhubungan dengan komputer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3) Delik-delik yang bermuatan pornografi anak (*content-related offences, child pornography*);
4) Delik-delik yang berhubungan dengan hak cipta (*offences related of infringements of copyrights*).

Berbagai perbuatan diatas menjadi sandaran untuk menilai pengaturan dalam UU ITE dan menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut.

METODE

Penelitian ini adalah penelitian hukum (*legal research*) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang Hak Cipta, khususnya yang terkait dengan karya cipta di bidang Komputer. Dalam penelitian ini akan dikaji dan dianalisis secara mendalam keterkaitan antara teori yang melandasi prinsip-prinsip perlindungan hukum, dihubungkan dengan ketentuan-ketentuan sebagaimana yang diatur dalam undang-undang hak cipta. Penelitian ini termasuk dalam kategori tipe penelitian normative atau *Normative Legal Research*. Pendekatan yang digunakan dalam penelitian ini adalah: *statuta approach*, *conseptual approach*, dan *comparative approach*. Teknik analisis yang digunakan adalah penalaran dan

argumentasi hukum untuk menjawab isu-isu penelitian yang diajukan sesuai dengan pendekatan yang digunakan.

HASIL DAN PEMBAHASAN

Upaya penanggulangan dan pencegahan kejahatan dapat dilakukan melalui suatu kebijakan kriminal (*criminal policy*) dengan menggunakan sarana "penal" (hukum pidana) dan sarana "non penal". (Laksana, 2019) Sarana penal dikenal dengan kebijakan/politik hukum pidana (*penal policy*). Menurut Sudarto, politik hukum pidana adalah usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang. (Sudarto, 1983) Sementara menurut Marc Ancel, *penal policy* adalah suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik. (Ramadhani et al., 2012)

Terkait dengan upaya penanggulangan *cybercrime* dengan menggunakan hukum pidana, telah ada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Tulisan ini akan melihat sejauhmana regulasi ini mampu memberikan peran dalam penanggulangan *cybercrime* di Indonesia. Mulai dari sistem perumusan tindak pidana sampai dengan sistem sanksi pidananya.

Undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE) ini diundangkan pada tanggal 21 April 2008 dalam Lembaran Negara Nomor 58. Dalam sejarahnya, kebijakan hukum pidana sebagai sarana penanggulangan *cybercrime* selama ini masih tersebar diberbagai peraturan perundang-undangan yang lebih bersifat sektoral dan memiliki keterbatasan, misalnya dalam Undang-Undang Telekomunikasi dan Undang-Undang Pers. Keluarnya Undang-Undang Nomor 11 tahun 2008 ini diharapkan mampu menjawab segala tantangan hukum dalam penanggulangan *cybercrime* di Indonesia.

a. Tindak Pidana dalam UU ITE

Ketentuan tindak pidana dalam UU ITE diatur dalam Bab XI dari Pasal 45 s/d Pasal 52. Adapun unsur-unsur tindak pidana dalam ketentuan pidana tersebut adalah :

1) Pasal 45 ayat (1) jo Pasal 27 ayat (1), (2), (3) atau (4) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Pasal 45 ayat (1) jo Pasal 27 ayat (2) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian
3) Pasal 45 ayat (1) jo Pasal 27 ayat (3) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4) Pasal 45 ayat (1) jo Pasal 27 ayat (4) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
5) Pasal 45 ayat (2) jo Pasal 28 ayat (1) : menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
6) Pasal 45 ayat (2) jo Pasal 28 ayat (2) : menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).
7) Pasal 45 ayat (3) jo Pasal 29 : mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
8) Pasal 46 ayat (1) jo Pasal 30 ayat (1) : mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun
9) Pasal 46 ayat (1) jo Pasal 30 ayat (2) : mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik
10) Pasal 46 ayat (1) jo Pasal 30 ayat (3) : mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

11) Pasal 47 jo Pasal 31 ayat (1) : melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain.
12) Pasal 47 jo Pasal 31 ayat (2) : 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.
13) Pasal 48 ayat (1) jo Pasal 32 ayat (1) : 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.
14) Pasal 48 ayat (1) jo Pasal 32 ayat (2) : dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
15) Pasal 48 ayat (1) jo Pasal 32 ayat (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.
16) Pasal 49 ayat (1) jo Pasal 33 : melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
17) Pasal 50 jo Pasal 34 ayat (1) : memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :

a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

18) Pasal 51 ayat (1) jo Pasal 35 : 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.

19) Pasal 51 ayat (2) jo Pasal 36 : melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

20) Pasal 52 ayat (1) : Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

21) Pasal 52 ayat (2) : Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

22) Pasal 52 ayat (3) : Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

23) Pasal 52 ayat (4) : Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Rumusan ketentuan pidana dalam undang-undang ITE menyebutkan secara tegas adanya unsur *"sifat melawan hukum"* yang terlihat pada rumusan "*tanpa hak atau melawan hukum*". Sebenarnya tanpa disebutkan/ditegaskan, pada prinsipnya setiap delik harus dianggap

bertentangan dengan hukum, sebagaimana ide dasar yang terkandung dalam Pasal 11 ayat (3) Konsep KUHP 2005. Sementara rumusan '*dengan sengaja*' juga dicantumkan secara tegas, sehingga jelas ada unsur kesengajaan (*dolus*) yang berarti menganut asas kesalahan atau *asas culpabilitas*. Sama halnya dengan sifat melawan hukum, pada prinsipnya tindak pidana melalui unsur-unsurnya dilakukan dengan kesengajaan kecuali dinyatakan secara tegas sebagai kealpaan. Hal ini sebagaimana ide dasar yang terkandung dalam Konsep KUHP 2005 Pasal 39 ayat (2).

Beberapa bentuk kriminalisasi dalam ketentuan pidana di atas diantaranya melalui dunia maya melakukan tindak pidana kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan/pengancaman, menyebarkan berita bohong dan informasi yang bermuatan SARA, mengakses data orang lain tanpa hak, atau menjebol sistem keamanan pihak lain. (Koto, 2021) (Qamar & Aswari, 2018) Disamping itu ada pula kriminalisasi yang mengandung pemberatan pidana, seperti tindak pidana kesusilaan terhadap anak dalam Pasal 27 ayat (1) Pidananya ditambah sepertiga dari pidana pokoknya. Begitu pula bagi korporasi yang melakukan tindak pidana dalam Pasal 27 sampai dengan Pasal 37 pidana pokoknya ditambah dua pertiga.

Gambar 1. Alur Persidangan Perkara Pidana

b. Sistem Pertanggungjawaban Pidana

Pertanggungjawaban pidana dalam Undang-Undang ITE dapat dijatuhkan kepada *individu* dan *korporasi.* Hal ini terlihat dari subjek tindak pidana yang terkandung dalam ketentuan pidananya, yaitu setiap orang. Pengertian orang dalam Ketentuan Umum Pasal 1 ayat (21) adalah *orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum*. Bahkan secara eksplisit, pertanggungjawaban korporasi dalam tindak pidana UU ITE disebutkan secara tegas dalam Pasal 52 ayat (4).

Dalam Undang-Undang ITE, korporasi juga merupakan subjek tindak pidana. Maka seharusnya diatur pula sistem pertanggungjawaban korporasi yang jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan. Namun dalam undang-undang ini justru tidak diatur mengenai tiga hal pokok tersebut. Terkait sanksi pidana misalnya, hanya disebutkan pidana pokoknya ditambah dua pertiga. Tidak diatur jenis sanksi lain yang lebih tepat bagi korporasi, seperti tindakan tata tertib penutupan sementara atau selamanya.

Ketentuan pidana dalam Undang-Undang ITE menganut sistem perumusan alternatif-kumulatif. (N. Setiawan et al., 2018) Hal ini terlihat dengan digunakannya rumusan "…*dan/atau*…", kecuali pada Pasal 52 yang sifatnya mengandung pemberatan pidana. Sementara untuk jenis sanksi *(strafsoort)* pidananya ada 2 (dua) jenis, yaitu pidana penjara dan pidana denda. Kedua jenis sanksi tersebut diancamkan untuk semua jenis kejahatan, baik dilakukan oleh individu maupun korporasi. Padahal terhadap korporasi tentunya tidak dapat dikenakan pidana penjara. Ditetapkannya korporasi sebagai subjek tindak pidana, seyogyanya hanya diancam pidana denda dan pidana tambahan/administrasi/tindakan tata tertib. Adapun Sistem perumusan jumlah/lamanya pidana (*strafmaat*) dalam Undang-Undang ITE adalah sistem maksimum khusus, yaitu maksimum khusus untuk pidana penjara berkisar antara 6 tahun sampai dengan 12 tahun dan maksimum khusus untuk pidana denda berkisar antara Rp 600.000.000,- sampai dengan Rp 12.000.000.000,-

KESIMPULAN

Bentuk upaya penanggulangan cybercrime atau kejahatan di bidang komputer dengan menggunakan sarana penal adalah dengan menggunakan kebijakan/politik hukum pidana (*penal policy*) yang lebih sesuai dengan keadaan dan situasi pada suatu saat sekarang dan untuk masa-masa yang akan datang. Oleh karena itu dibentuklah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal ini dimaksudkan untuk mengatasi permasalahan sebelumnya terkait dengan pengaturan tentang penanggulangan *cybercrime* yang masih tersebar diberbagai peraturan perundang-undangan yang berlaku. Pengaturan tersebut lebih bersifat sektoral dan memiliki keterbatasan, misalnya dalam Undang-Undang Telekomunikasi dan Undang-Undang Pers. Pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik dapat dijatuhkan kepada *individu* dan *korporasi.* Namun demikian sistem pertanggungjawaban korporasi belum cukup jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan.

DAFTAR RUJUKAN

Arief, B. N. (2006). *Tindak pidana mayantara : perkembangan kajian cyber crime di Indonesia*. RajaGrafindo Persada. https://opac.perpusnas.go.id/DetailOpac.aspx?id=403380

Aswari, A. (2020). Perlindungan Hukum Tanpa Penegakan Hukum Dalam Sengketa Transaksi Elektronik. *Kertha Patrika*, *42*(2), 163. https://doi.org/10.24843/kp.2020.v42.i02.p05

Golubev, V. (2012). Cyber-crime and legal problems of Internet usage. *Zaporizhia Law Institute, Ministry of Interior of Ukraine*, *11*(2).

Keyser, M. (2017). The council of europe convention on cybercrime. In *Computer Crime* (pp. 131–170). Taylor and Francis. https://doi.org/10.4324/9781315095493-7/COUNCIL-EUROPE-CONVENTION-CYBERCRIME-MIKE-KEYSER

Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS)*, *2*(2), 103–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs/article/view/124

Laksana, A. W. (2019). PEMIDANAAN CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA POSITIF. *Jurnal Hukum*, *35*(1), 52–76. https://doi.org/10.26532/JH.V35I1.11044

Middin, M. A., Salle, S., & Aswari, A. (2021). Menakar Faktor Penghambat Dalam Mewujudkan Kepastian Hukum Dibidang Pertanahan. *PLENO JURE*, *10*(2), 115–121. https://doi.org/10.37541/PLENOJURE.V10I2.608

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional. *Jurnal Ilmu Hukum Jambi*, *5*(2), 43297. https://www.neliti.com/publications/43297/

Qamar, N., & Aswari, A. (2018). Healing or Hurting: Development of Highway Public transportation Technology. *Jurnal Dinamika Hukum*, *18*(3), 319–328. https://doi.org/10.20884/1.JDH.2018.18.3.2144

Rahim, A., & Rahim, M. I. F. (2021). Pemalsuan Surat dalam Arti Formil dan Materil Beserta Akibat Hukumnya. *Pleno Jure*, *10*(2), 68–80. https://doi.org/10.37541/plenojure.v10i2.575

Ramadhani, G. S., Arief, B. N., & Purwoto, P. (2012). Sistem Pidana dan Tindakan "Double Track System" Dalam Hukum Pidana di Indonesia. *Diponegoro Law Journal*, *1*(4), 1–9. https://ejournal3.undip.ac.id/index.php/dlr/article/view/612

Sari, N. W. (2019). KEJAHATAN CYBER DALAM PERKEMBANGAN TEKNOLOGI INFORMASI BERBASIS KOMPUTER. *Jurnal Surya Kencana Dua : Dinamika Masalah Hukum Dan Keadilan*, *5*(2). https://doi.org/10.32493/SKD.V5I2.Y2018.2339

Setiawan, A., Shahroom, A., Huang, T., & Zahidah, N. S. (2016). The Complexities Of Programme Management: Case Study Of Trans-Asean Gas Pipeline. *PM World Journal*, *5*(5). https://pmworldlibrary.net/wp-content/uploads/2016/05/pmwj46-May2016-Complexities-of-

Programme-Management-Trans-ASEAN-Gas-Pipeline-case-study.pdf

Setiawan, N., Emia Tarigan, V. C., Sari, P. B., Rossanty, Y., Putra Nasution, M. D. T., & Siregar, I. (2018). Impact of cybercrime in e-business and trust. *International Journal of Civil Engineering and Technology*, *9*(7), 652–656. https://www.researchgate.net/profile/Nashrudin-Setiawan/publication/327335383_Impact_of_cybercrime_in_e-business_and_trust/links/60559c8f92851cd8ce52afe8/Impact-of-cybercrime-in-e-business-and-trust.pdf

Sudarto, S. (1983). *Hukum pidana dan perkembangan masyarakat : kajian terhadap pembaharuan hukum pidana*. Sinar Baru. https://opac.perpusnas.go.id/DetailOpac.aspx?id=611849

Sutarwan, H., Widiana, I. G., & Amin, I. (2007). *Cyber crime : modus operandi dan penanggulangannya*. LaksBang PRESSindo. https://opac.perpusnas.go.id/DetailOpac.aspx?id=874110

Wahid, A. (2005). *Kejahatan mayantara (Cyber crime)*. Refika Aditama. http://library.stik-ptik.ac.id

Wahyudi, I. (2006). *Kebijakan Pidana Terhadap Kejahatan Mayantara*. Universitas Riau.

WidyoPramono, W. (1994). *Kejahatan di bidang komputer*. Pustaka Sinar Harapan. https://opac.perpusnas.go.id/DetailOpac.aspx?id=271093

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63–74. https://doi.org/10.15294/ijcls.v5i1.23273