Jurnal Magister Hukum
ARGUMENTUM

Volume 2, Nomor 1, Maret 2017 ISSN 25284584

ARGUMENTUM
Jurnal Berkala Magister Ilmu Hukum
Fakultas Hukum Universitas Surabaya
ISSN 25284584

Diterbitkan oleh Program Studi Magister Ilmu Hukum
Fakultas Hukum Universitas Surabaya
Dua kali setahun pada bulan Maret dan Oktober
Volume 2, Nomor 1, Maret 2017

Alamat Sekretariat ARGUMENTUM:
Program Studi Magister Ilmu Hukum Fakultas Hukum Universitas Surabaya
Jalan Raya Kalirungkut, Surabaya 60293
T: 031-2981223; 1225
F: 031-2981121
E: hukum@ubaya.ac.id atau wisnu@staff.ubaya.ac.id

EDITORIAL

Mengucap syukur kepada Tuhan Yang Maha Pandai, Jurnal Magister Hukum Program Studi Magister Ilmu Hukum fakultas Hukum Universitas Surabaya kembali hadir pada bulan Maret 2017. Kami mengucapkan terimakasih kepada para mahasiswa S-2 maupun S-3 yang berkontribusi dalam jurnal ini, juga bapak dan ibu dosen yang telah berpartisipasi dalam menulis. Pada Volume 2 Nomor 1 Maret 2017 ini ada empat (4) hasil penelitian mahasiswa S-2 yang dipublikasikan, antara lain: Imma Noer Fatimah yang mengungkapkan hasil penelitiannya tentang "Pengajuan Keberatan atas Putusan Komisi Pengawas Persaingan Usaha dan Implikasi Hukumnya".Dilanjutkan dengan Mohammad Donny Aprianto Wibowo dengan judul "Pengaruh Pemeriksaan Persiapan terhadap Obyektifitas Hakim Pengadilan Tata Usaha Negara dalam Menyelesaikan Sengketa Tata Usaha Negara". Kemudian, hasil penelitian mengenai "Politik Hukum Ikrar Cerai Talak di Depan Pengadilan" ditulis oleh Rio Firdaus. Diakhiri dengan hasil penelitian dari Steven Mandraguna yang menyoroti tentang "Persetujuan Pekerja/Buruh sebagai suatu Alasan Penghapus Pidana dalam Perbuatan Pengusaha pada suatu Usaha Dagang yang Tidak Memenuhi Ketentuan Pengupahan". Dosen yang juga mahasiswa S-3 pada Sekolah Pascasarjana Program Doktor FH-UGM, Hwian Christianto, tertarik untuk menulis tentang "Kajian FilsafatPerbuatan Pornografi Internet (Cyberporn)" dan dilanjutkan oleh Nabbilah Amir yang meneliti tentang "Aspek Hukum Tata Ruang dalam Pengelolaan Wilayah Pesisir dan Pulau-Pulau Kecil oleh Pemerintah Daerah". Nur Latifah Hanum menulis mengenai "Keberadaan Mahkamah Konstitusi dalam Struktur Kelembagaan Negara di Indonesia". Terakhir, Anton Hendrik menjelaskan tentang "Membanding Perbuatan yang Dilarang dalam UU ITE dan Konvensi Internasional: Penanggulangan Tindak Pidana Siber." Dengan terbitnya jurnal ARGUMENTUM yang kedua ini, kami berharap semakin banyak hasil penelitian mahasiswa dan dosen, serta tulisan-tulisan lepas dosen-dosen hukum yang dapat dipublikasikan melalui jurnal ini agar dapat memberikan pencerahan dan pengetahuan kepada masyarakat.

Surabaya, Maret 2017
Redaksi

Membanding Perbuatan yang Dilarang dalam UU ITE dan Konvensi Internasional: Penanggulangan Tindak Pidana Siber

Anton Hendrik S., S.H., M.H.*

ABSTRACT

Information technology development changes human culture of living. Beside positive impact, it also brings challenges, problems, and threats. The behavior of pursuing profit in illicit ways also following the development as the new media. Indonesia criminalized the illicit behavior regarding the technology development in 2008 through Law 11/2008 and in 2016 the law was amended by Law 19/2016. The criminalization is expected to be a better new types of crime deterrence. Some of the norms adopted from international convention. This paper discusses the regulation of criminalized behavior in *Convention on Cybercrime*, Law 11/2008, and Law 19/2016.

Keywords: Criminalization, criminalized behavior, convention, Law 11/2008, Law 19/2016.

PENDAHULUAN

Perkembangan teknologi yang berujung pada kemudahan hidup manusia juga membawa dampak negatif karena demikian halnya kejahatan *co-evolve* dengannya. Berkat konvergensi telematika, sekarang teknologi sudah menggabungkan cara kerjanya dengan jaringan dan juga telekomunikasi, sehingga hampir segala sesuatu dapat diakses menggunakan perangkat yang kita gunakan.

Komputer perkembangannya ke arah semakin canggih, semakin kecil ukurannya. Komputer bekerja didukung dari sinergi antara perangkat keras dan perangkat lunak. Semua sistem dalam computer bekerja untuk mengolah data, mulai dari pembacaan data melalui *input device*, hasil olahan data yang dapat disimpan dalam *storage*, sampai pemindahan hasil olahan data melalui *output device*. Pengguna komputer dapat memanipulasi data dan memberi

* Dosen Tetap Fakultas Hukum Universitas Surabaya

perintah melalui *keyboard, mouse,* layar sentuh, dan lain semacamnya.[1] Dalam melakukan pekerjaannya, komputer juga dapat disambungkan dengan perangkat-perangkat lain yang kompatibel dengannya seperti scanner, kamera, printer, *usb disk,* tv, proyektor, mobile device, dan lain semacamnya.[2]

Internet merupakan akronim dari *interconnected networks.* Internet merupakan jaringan global yang menghubungkan perangkat-perangkat, termasuk komputer dan mobile phone, untuk akses dan pertukaran data menggunakan infrastruktur telekomunikasi. Ini yang membuat dunia global menjadi sangat terjangkau. Dunia yang luas seolah tampak seperti desa yang kecil, seperti yang dinyatakan Marshall McLuhan bahwa dunia sudah menjadi desa berkat pengaruh teknologi elektronik dan informasi yang sangat cepat bergulir bahkan instan seketika itu juga di dunia.[3] Internet yang menyambungkan semua perangkat teknologi elektronik itulah yang memungkinkan hal ini terjadi. Internet merupakan hasil konvergensi antara jaringan, perangkat dan telekomunikasi.[4]

Perkembangan dalam hal konvergensi tersebut telah merubah pola hidup manusia. Semua kemudahan yang disebabkannya dibarengi dengan munculnya perbuatan-perbuatan tercela yang dilakukan menggunakan teknologi informasi yang terkonvergensi tersebut dan yang ditujukan kepada sistem teknologi informasi tersebut. Terlebih lagi penelusuran identitas pelaku perbuatan tercela tersebut bagi proses penegakan hukum bukanlah sesuatu yang mudah, mengingat tidak ada penampakan fisik sama sekali. Yang ada hanyalah alamat *internet protocol* (IP Address), yang sekarang ini juga sudah banyak sekali jasa yang dapat menyembunyikan IP Address untuk kepentingan tertentu, seperti contohnya hidemyass, ultrasurf, dan Virtual

---

[1] Widyopramono dalam Petrus R. Golose, *Seputar Kejahatan Hacking: Teori dan Studi Kasus,* Yayasan Pengembangan Kajian Ilmu Kepolisian: Jakarta, 2008, h.6
[2] *Ibid.*
[3] Marshall McLuhan, *Understanding Media,* Gingko Press: California, 2003, h.6
[4] Makarim, Edmon, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian,* Raja Grafindo Persada: Jakarta, 2005, h. 6

Private Network (VPN). Padahal jika dianalogikan, "wajah" dari setiap orang yang berkomunikasi menggunakan protocol internet adalah IP Address. Namun sekarang "wajah" tersebutpun di dunia maya bisa disembunyikan menggunakan "topeng". Itu membuat pelaku kejahatan siber semakin sulit terlacak.

PEMBAHASAN

Kriminalisasi Tindak Pidana Siber dalam Masyarakat Internasional dan dalam *Convention on Cybercrime*, Budapest

Aturan-aturan hukum pidana yang telah ada sebelumnya, tidak semua dapat menanggulangi perkembangan tindak pidana yang berkaitan dengan media siber. Sehingga tidak semua penjahat siber dapat dihukum. Kejahatan siber diungkapkan oleh Susan Brenner sebagai *'new wine in new bottle'* dan juga sekaligus *'old wine in a new bottle'*.[5] Ada tipe kejahatan konvensional yang dilakukan menggunakan sarana media siber, namun ada juga kejahatan yang benar-benar baru karena munculnya konvergensi telematika.

Untuk menghadapi ancaman dan bahaya dari tindak pidana siber, beberapa organisasi internasional melakukan kajian dan pertemuan ilmiah yang membahas tindak pidana ini. Beberapa di antaranya adalah *Organisation for Economic Cooperation and Development (OECD), United Nations (UN), The Group of Eight (G8),* dan *Council of Europe (CoE)*.[6]

Suatu hukuman dapat dijatuhkan apabila perbuatan yang patut dihukum tersebut sudah ada pengaturannya dalam undang-undang.[7] Harus ada pernyataan dari undang-undang, bahwa suatu perbuatan tercela tersebut

---

[5] Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, Virginia Journal of Law and Technology, Vol. 9 No. 13, University of Virginia, 2004

[6] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama: Bandung, 2012, h.102

[7] Asas Legalitas, yang dalam bahasa latin: *Nullum delictum nulla poena sine praevia lege poenali*, yang artinya tidak ada tindak pidana, tidak ada sanksi pidana, tanpa ada ketentuan pidana yang mengatur sebelumnya.

masuk dalam kategori tindak pidana, agar perbuatan tercela tersebut dapat dihukum. Dari perbuatan tercela secara sosial kemasyarakatan namun tidak dicela oleh hukum dijadikan tercela oleh hukum dan diberi label tindak pidana, itulah yang dinamakan dengan kriminalisasi.

Komunitas internasional melihat bahaya dari kejahatan menggunakan komputer sejak 1980. Seperti contohnya negara-negara di Eropa dan Amerika Utara pada kisaran tahun 1980-an yang mulai melakukan kriminalisasi terhadap perbuatan-perbuatan yang dulu dapat dikatakan 'baru' dalam melakukan tindak pidana konvensional yaitu menggunakan teknologi komputer dalam melakukannya. Yang kemudian pada tahun 1990-an, negara-negara di dalam kedua wilayah tersebut mengadopsi hukum yang meng-kriminalisasi tindakan-tindakan yang termasuk mengakses sistem computer tanpa hak, merusak data di dalam sistem komputer dan melepas *malware*.[8]

Sebagai kulminasi dari upaya-upaya kriminalisasi untuk menanggulangi tindak pidana siber, OECD melakukan studi untuk harmonisasi hukum nasional untuk tindak pidana siber. Di kisaran waktu yang hampir bersamaan CoE juga memulai memelajari isu yang sama, yang berujung pada *Convention on Cybercrime*.[9] Namun menurut Marjie Britz, OECD lebih tepatnya mensponsori komite ad-hoc yang bernama *Committee of Experts on Computer-Related Crime of the Council of Europe* yang dibentuk antara 1983 dan 1985, dan komite tersebut yang melakukan tersebut.[10] Saran kriminalisasi dari komite tersebut adalah (garis bawah dari penulis):

1. *Any manipulation of data which is intended to commit illegal transfer of funds or other valuables*
2. *Any manipulation of data intended to commit forgery*

---

[8] Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, dalam Jack M. Balkin et al., *Cybercrime: Digital Cops in a Networked Environment*, New York University Press: New York, 2007, h. 207

[9] Lihat Council of Europe, *583 Meeting of the Ministers' Deputies*, February 4, 1997, Appendix 13, http://www.m-cc.int/dec/1997/583/2a13.html, dalam Jack M. Balkin et al., *Op.cit.*

[10] Marjie T. Britz, *Computer Forensics and Cyber Crime: An Introduction*, Third Edition, Pearson Education Inc.: New Jersey, 2013, h.208

3. *Any manipulation intended to interfere with the functioning of a computer or other telecommunications system*
4. *Any incident of software theft or software piracy*
5. *Any unauthorized access or interception of another's computer with malicious intent.*[11]

Komite yang sama yang terbentuk pasca sponsor OECD, menyajikan dua daftar perbuatan-perbuatan yang perlu dikriminalisasi. Daftar yang pertama adalah saran yang bersifat opsional untuk dikriminalisasi, yaitu:

1. ***The alteration of computer data or computer programs***—*the alteration of computer data or computer programs without rights.*
2. ***The practice of computer espionage***—*the acquisition by improper means or the disclosure, transfer, or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.*
3. ***The unauthorized use of a computer***—*the use of a computer system or network without right that either (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning.*
4. ***The unauthorized use of a protected computer program***—*the use without the right of a computer program which is protected by law and which has been reproduced without right, with the intent either to procure an unlawful economic gain for oneself or for another person or to cause harm to the holder of the right.*[12]

Daftar yang kedua, menyarankan perbuatan-perbuatan yang harus dikriminalisasi oleh negara-negara peserta, yaitu:

1. ***Computer fraud***—*the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing, thereby causing economic or possessory loss of property of another*

---

[11] *Ibid.*

[12] United Nations (2000). "*United Nations Manual on the Prevention and Control of Computer-Related Criteria.*" International Review of Criminal Policy, 43 & 44. Dalam Marjie T. Britz, *Ibid.*

person with the intent of procuring an unlawful economic gain for oneself or for another person.

2. ***Computer forgery****—the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offense of forgery if it had been committed with respect to a traditional object of such an offense.*
3. ***Damage to computer data or computer programs****—the erasure, damaging, deterioration, or suppression of computer data or computer programs without right.*
4. ***Computer sabotage****—the input, alteration, erasure, or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or telecommunications system.*
5. ***Unauthorized access****—the access without right to a computer system or network by infringing security measures.*
6. ***Unauthorized interception****—the interception made without right and by technical means, or communications to, from and within a computer system or network.*
7. ***Unauthorized reproduction of a protected computer program****—the reproduction, distribution, or communication to the public without right of a computer program which is protected by law.*
8. ***Unauthorized reproduction of a topography****—the reproduction without right of topography protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography.*[13]

Sejak itu PBB mengadakan kongres yang membahas tentang computer related crime yang dimulai pada kongres ke delapannya, *UN Congress on the Prevention of Crime and Treatment of Offender* di Havana, Cuba pada tahun 1990 sampai dengan kongresnya yang ke-12 di Brazil pada tahun 2010.

CoE pada tanggal 23 November 2001 mengadakan konferensi yang menghasilkan *Convention on Cybercrime* di Budapest. Konvensi ini diadakan untuk menentukan pembedaan karakteristik tindak pidana siber. Tentang perbuatan yang dicela oleh konvensi ini, dibagi menjadi empat kategori:

[13] *Ibid.*

- *Offences against the confidentiality, integrity and availability of computer data and systems* (Pasal 2-Pasal 6)
- *Computer-related offences* (Pasal 7-Pasal 8)
- *Content-related offences* (Pasal 9)
- *Offences related to infringements of copyright and related rights* (Pasal 10)

Dalam Pasal 2 konvensi ini perbuatan yang dilarang adalah:

> *"...committed intentionally, the access to the whole or any part of a computer system without right... committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Pasal ini meminta setiap negara anggota peserta konvensi untuk mengadopsi atau membuat hukum yang melarang *illegal access*. Dijelaskan juga bahwa *illegal access* tersebut merupakan perbuatan mengakses sebagian atau keseluruhan sistem komputer tanpa ada alas hak, dengan membobol sistem keamanannya, dengan tujuan mendapatkan data komputer atau tujuan tidak jujur yang lain.

Dalam Pasal 3 konvensi ini mengatur perbuatan yang dilarang dalam hal intersepsi ilegal:

> *"...committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data... committed with dishonest intent, or in relation to a computer system that is connected to another computer system."*

Intersepsi juga bisa diterjemahkan dengan penyadapan, namun dalam hal ini yang disadap adalah transmisi data komputer non-publik (yang sifatnya tidak untuk disebarluaskan untuk umum), termasuk emisi elektromagnetik dari komputer yang membawa data komputer. Intersepsi ini dapat dilakukan melalui atau dari dalam sistem komputer oleh karena itu dicantumkan dalam ketentuan pasal.

Pasal 4 mengatur perbuatan yang dilarang yaitu:

> *"...committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."*

Pasal ini berkaitan dengan perusakan, penghapusan, perubahan, penahanan/penyembunyian data secara sengaja dan tanpa hak.

Pasal 5 mengatur tentang perbuatan:

> *"...committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."*

Jika Pasal 4 mengatur tentang manipulasi data komputer tanpa hak, Pasal 5 melarang tindakan mengganggu fungsi sistem komputer dengan cara memanipulasi data komputer. Jadi Pasal 5 ini mengandung unsur adanya akibat yang dicela, bukan hanya perbuatannya.

Pasal 6 mengatur larangan tentang penguasaan, perbuatan produksi, penjualan, pengadaan, impor, distribusi, yang pada intinya membuat perangkat (lunak maupun keras) yang digunakan untuk melakukan tindak pidana siber yang diatur dalam Pasal 2-5. Selain perangkat, penguasaan, perbuatan produksi, penjualan, pengadaan, impor, distribusi atau membuat password komputer, kode akses yang digunakan untuk mengakses sistem komputer dengan tujuan melakukan tindak pidana yang dimaksud dalam Pasal 2-5. Pasal 6 isinya:

> *"....committed intentionally and without right:*
>
> *a. the production, sale, procurement for use, import, distribution or otherwise making available of:*
>
> *i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;*
>
> *ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,*

with intent that it be used for the purpose of committing dny of the offences established in Articles 2 through 5; and

b. *the pcssession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

Namun di ayat 2-nya, Pasal 6 ini juga menjelaskan bahwa jika perbuatan pengadaan dan lain semacamnya ini digunakan untuk mencoba keamanan sistem komputer, maka perbuatan tersebut tidak akan disebut sebagai tindak pidana.

Pasal 7 Convention on Cybercrime mengatur tentang pemalsuan terkait dengan komputer. Isinya:

> *"...committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible."*

Perbuatan sengaja dan tanpa hak memasukkan, mengubah, menghapus, atau menahan data komputer yang menghasilkan data palsu dengan tujuan digunakan untuk keperluan berkaitan dengan hukum agar seolah-olah data komputer tersebut sah, harus dilarang.

Pasal 8 konvensi ini mengatur tentang penipuan yang berkaitan dengan komputer. Isi pasal:

> *"...committed intentionally and without right, the causing of a loss of property to another person by:*
>
> a. *any input, alteration, deletion or suppression of computer data;*
> b. *any interference with the functioning of a computer system,*
>
> *with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."*

Pasal ini melarang perbuatan sengaja dan tanpa hak yang menyebabkan hilangnya properti milik orang lain melalui:

- input data, perubahan, penghapusan atau penahanan/penyembunyian data komputer
- setiap gangguan terhadap fungsi sistem komputer

yang dengan maksud jahat dan curang mengambil keuntungan dari orang lain tanpa hak.

Pasal 9 konvensi ini mengatur tentang tindak pidana siber yang terkait dengan pornografi anak. Pengaturannya cukup luas, mulai dari produksi menggunakan sistem komputer, menawarkan, mengunggah, mendistribusi, transmisi, mengambil, mengunduh, menguasai data komputer atau sistem komputer yang bermuatan pornografi anak.

Pasal 10 mengatur tentang tindak pidana terkait pelanggaran hak cipta. Pengaturannya merujuk pada *Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty,* namun bergantung pada hukum masing-masing negara terkait hak cipta dan hak-hak lain yang terkait.

Dilihat dari setiap pengaturan tentang perbuatan yang dilarang, dapat disimpulkan bahwa *cybercrime* dapat dikategorikan menjadi dua:

1) Tindak pidana terhadap sistem komputer/elektronik
2) Tindak pidana yang menggunakan sarana sistem komputer/ elektronik

Namun di dalam konvensi tidak ada pengaturan tentang hukuman yang dijatuhkan pada perbuatan yang telah dikriminalisasi, karena konvensi hanya mengharuskan negara-negara peserta konvensi untuk mengadopsi atau membuat aturan hukum yang mencela perbuatan sebagai tindak pidana. Setiap sanksi ditentukan oleh masing-masing negara yang mengkriminalisasi tindak pidana siber.

Perbuatan yang dilarang dalam UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan UU No. 19 Tahun 2016 Tentang Perubahan UU ITE

Di Indonesia, rezim hukum siber dimulai sejak diberlakukannya Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).[14] UU ITE dapat dikategorikan sebagai undang-undang beraspek pidana. Perbuatan yang dilarang diatur dalam Bab VII mulai Pasal 27 sampai dengan Pasal 37.

Dapat dilihat bahwa pasal-pasal dalam UU ITE, sebagian ketentuan ada yang mengadopsi dari konvensi internasional sebagaimana dijelaskan di atas, namun disajikan dengan sistematika yang berbeda.

Pasal 27 UU ITE berisi ketentuan:

1	Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan	yang melanggar kesusilaan.
2		perjudian.
3		penghinaan dan/atau pencemaran nama baik.
4		pemerasan dan/atau pengancaman.

Pasal 27 ini masuk dalam kategori *cybercrime* yang *'old wine, new bottle'*. Perbuatan yang dilarang dalam pasal ini intinya tentang distribusi dan/atau transmisi dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik secara tanpa hak, namun isi konten berbeda sesuai yang diatur per ayatnya. Mengenai definisi dari perbuatan 'disribusi' dan 'transmisi', dijelaskan lebih lanjut dalam perubahan UU ITE yaitu Undang-undang No. 19 Tahun 2016 tentang Perubahan Undang-undang No. 11 Tahun

[14] Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58

2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut Perubahan UU ITE).[15] Demikian dalam Penjelasan Pasal 27 ayat 1-nya:

> "Yang dimaksud dengan "mendistribusikan" adalah mengirimkan *dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen* Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik.
> Yang dimaksud dengan "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/atau Dokumen Eletronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.
> Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik."

Mengenai muatan melanggar kesusilaan, untuk proposisi "kesusilaan" yang dimaksud dalam ayat 1, UU ITE tidak memberi penjelasan. Sama halnya di dalam Undang-undang No. 44 Tahun 2008 tentang Pornografi. Dengan demikian konsep kesusilaan kembali ke KUHP sebagai *lex generali*. Di KUHP, tindak pidana kesusilaan diatur dalam Bab XIV dengan judul bab "Kejahatan Terhadap Kesusilaan". Di KUHP-pun proposisi ini terbuka untuk ditafsirkan. R. Soesilo menjelaskan bahwa arti kesusilaan (*zeden, eerbaarheid*) adalah perasaan malu yang berhubungan dengan nafsu kelamin misalnya bersetubuh, meraba buah dada perempuan, meraba tempat kemaluan wanita, memperlihatkan anggota kemaluan, mencium, dan semacamnya.[16] Sehingga setiap tindakan mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan tersebut secara sengaja dan tanpa hak, dapat dihukum.

---

[15] Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251

[16] R. Soesilo, *Kitab Undang-undang Hukum Pidana Serta Komentar-komentarnya Lengkap Pasal Demi Pasal*, Politeia: Bogor,1996, h.204

Mengenai konten perjudian, proposisi "perjudian" pada ayat 2 juga tidak ada penjelasan dalam UU ITE. Di dalam KUHP tentang perjudian diatur dalam Pasal 303 dan Pasal 303bis. R. Soesilo menjelaskan apa saja yang masuk dalam permainan judi sebagai berikut: "...tiap-tiap permainan yang mendasarkan pengharapan buat menang pada umumnya bergantung pada untung-untungan saja,...".

Mengenai konten penghinaan dan/atau pencemaran nama baik, dijelaskan dalam Penjelasan Pasal 27 ayat 3 dalam Perubahan UU ITE bahwa *mengenai proposisi ini ikut konsep dalam KUHP. Pengaturan mengenai* penghinaan ada di Bab XVI tentang Penghinaan, pada Bab II (Pasal 134, Pasal 136bis, dan Pasal 137 /penghinaan terhadap Presiden atau Wakil Presiden)[17] dan Bab *VIII* (Pasal 207 /penghinaan terhadap penguasa umum) Buku Kedua KUHP. Bab XVI dapat dikatakan delik penghinaan secara umum, sedangkan yang terdapat di Bab II dan VIII dapat dikatakan sebagai penghinaan secara khusus. Konstruksi dasar "penghinaan" dapat kita lihat dalam Pasal 310 KUHP untuk unsur: "...menyerang kehormatan atau nama baik seorang, dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum...".

Untuk proposisi "*pemerasan dan/atau pengancaman" sama halnya,* harus merujuk pada KUHP. Di dalam Penjelasan Pasal 27 ayat 4 Perubahan UU ITE dinyatakan bahwa ketentuan pada ayat ini mengacu pada ketentuan pemerasan dan/atau pengancaman yang diatur dalam KUHP. Mengingat stelsel pengaturan yang digunakan dalam proposisi dalam Pasal 27 ayat 4 adalah 'dan/atau' yang berarti kumulatif-alternatif, artinya salah satu saja terpenuhi sudah cukup untuk memenuhi pelanggaran, asalkan unsur sebelumnya juga terpenuhi.

---

[17] Pasal 134, Pasal 136bis, dan Pasal 137 KUHP telah diputus bertentangan dengan UUD 1945 dan dinyatakan tidak mengikat secara hukum oleh Mahkamah Konstitusi.

Di dalam KUHP proposisi yang mirip dengan 'pemerasan dan/atau pengancaman' ada di Bab XXIII Buku Kedua, yaitu judul babnya sendiri "Pemerasan dan Pengancaman". Perihal 'ancaman', di dalam KUHP mengatur dua jenis, yaitu ancaman kekerasan dan ancaman lainnya. 'Ancaman lainnya' adalah ancaman pencemaran nama baik, ancaman membuka rahasia. Namun perlu dicatat bahwa setiap ancaman di dalam KUHP selalu ada tujuannya, berbeda halnya dengan Pasal 27 ayat 4 UU ITE yang tidak mengharuskan adanya tujuan.

Dilihat dari perbuatan yang dilarang dalam Pasal 27 ini sangat menggambarkan *content-related offense*. Tipe perbuatannya bukan kejahatan terhadap komputer, melainkan kejahatan yang terkait konten dalam media siber menggunakan sistem elektronik. Sanksi pidana untuk ketentuan Pasal 27 ini ada di Pasal 45 Perubahan UU ITE.

Pasal 28 UU ITE terdiri dari dua ayat, ayat pertama mengatur tentang penipuan yang berkaitan dengan transaksi elektronik dan ayat ke-dua tentang penyebar kebencian/SARA. Berikut kutipannya:

1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Sama halnya dengan Pasal 27, Pasal 28 ini juga masih mengatur perihal *content-related offense*. Ayat 1 kerap digunakan sebagai penanggulang tindak pidana penipuan melalui transaksi jual beli *online*, yang juga termasuk melindungi perorangan. Jika dilihat dari sistematika penyusunan pasal, benang merah dari pasal ini seharusnya adalah tentang isu publik, yaitu menanggulangi kekacauan publik. Dilihat dari karakteristik dari ayat 2 yang melarang perbuatan menyebarkan informasi elektronik yang muatannya

menyerang SARA. Namun di dalam Naskah Akademik perancangan UU ITE tidak ditemukan tentang informasi ini. Meskipun begitu, menggunakan metode penafsiran sudah cukup untuk menggunakan Pasal 28 ayat 1 UU ITE untuk menanggulangi tindak pidana penipuan *online*. Ancaman pidana untuk Pasal 28 UU ITE ini diatur dalam Pasal 45A ayat 1 Perubahan UU ITE.

Pasal 29 UU ITE mengatur tentang pengancaman kekerasan yang ditujukan secara pribadi. Berikut kutipannya:

> "Setiap Orang dengan sengaja dan tanpa hak mengirimkan *Informasi* Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. "

Tentang ancaman, sudah diatur juga di Pasal 27 ayat 4. Sehingga pasal ini seperti *redundancy*, karena sama-sama mengandung 'ancaman'. Perlu diketahui apakah ini adalah pengaturan pengulangan yang sia-sia atau tidak. Proposisi 'ancaman' dalam Pasal 29 menyebutkan secara eksplisit bahwa ancamannya adalah ancaman kekerasan, dengan alternatif perbuatan 'menakut-nakuti secara pribadi'. Ancaman hukumannya diatur dalam Pasal 45B Perubahan UU ITE.

Di UU ITE dan perubahannya, *Cybercrime* yang tergolong *'new wine, new bottle'* dimulai di Pasal 30 sampai dengan Pasal 35. Pasal 30 jo Pasal 46 UU ITE mengatur tentang akses ilegal (*illegal access*) yang dibagi menjadi tiga ayat. Yang menyatakan:

1		milik Orang lain dengan cara apa pun.	pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600.000.000,-
2	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer	dengan cara apa pun *dengan tujuan untuk* memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.	pidana penjara paling lama 7 tahun dan/atau denda paling banyak Rp700.000.000,-

3	dan/atau Sistem Elektronik	dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.	pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800.000.000,-

Kualifikasi perbuatan akses ilegal ini yaitu pada ayat 2 dan ayat 3. Ayat 2 dikualifikasi karena ada tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik, sedangkan pada ayat 3 yaitu tentang perbuatan dilakukan menggunan perusakan sistem pengamanan. Masing-masing kualifikasi memberikan pemberatan sanksi pidana dibandingkan sanksi pidana pada tindak pidana akses ilegal pada pokoknya di ayat 1.

Pasal 31 UU ITE mengatur tentang *illegal interception*.

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.

Penyadapan dalam terminologinya bisa diartikan sebagai *wire-tapping* atau *interception*. *Wire-tapping* lebih ke arah mencuri dengar atau mencuri rekam, sedangkan *interception* lebih ke arah mencuri transmisi. Dalam Penjelasan Pasal 31 ayat 1 Perubahan UU ITE dijelaskan yang dimaksud dengan "intersepsi atau penyadapan" lebih detil yaitu kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak

bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi. Ancaman pidananya diatur dalam Pasal 47 UU ITE.

Intersepsi tidak dikatakan sebagai ilegal apabila dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan dan institusi lain yang memiliki wewenang berdasar UU. Demi terjaminnya kepastian hukum, UU ITE memerintahkan agar tindakan intersepsi dalam rangka penegakan hukum ini diatur dalam UU.

Pasal 32 mengatur tentang tindak pidana yang sasarannya adalah informasi elektronik atau dokumen elektronik, yaitu:

- mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik secara sengaja, tanpa hak atau melawan hukum.
- 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.
- 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 33 dapat dikatakan sebagai aturan tentang *computer-system interference*, yaitu dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya. Ancaman pidananya diatur dalam Pasal 49 UU ITE.

Pasal 34 ayat 1 UU ITE merumuskan perbuatan yang dilarang:

> "...dengan sengaja dan tanpa hak atau melawan hukum 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."

Pasal ini mengatur tentang pelarangan penyediaan sarana bagi tindak pidana siber. Ancaman pidananya diatur dalam Pasal 50 UU ITE. Terdapat pengecualian untuk perbuatan yang dirumuskan dalam Pasal 34 ayat 1, yaitu apabila perbuatannya ditujukan untuk kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35 UU ITE melarang tindakan manipulasi data agar seolah tampak asli/otentik. Perbuatan yang dilarang adalah: 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. Untuk perbuatan ini ancaman hukumannya diatur dalam Pasal 51 ayat 1 UU ITE.

Pasal 36 UU ITE mengatur tentang pemberatan pidana. Pasal ini menekankan pada akibat dari setiap perbuatan yang dilarang dalam Pasal 27 sampai dengan Pasal 34 yang menimbulkan kerugian diancam dengan pidana yang lebih berat dari pada perbuatan yang tidak menimbulkan kerugian. Ancaman pidananya diatur dalam Pasal 51 ayat 2 UU ITE.

Pasal 37 memperluas ruang lingkup kriminalisasi. Perbuatan yang dilarang UU ITE yang dilakukan di luar yurisdiksi Indonesia, yang di negara lain mungkin tidak dipertimbangkan sebagai tindak pidana, apabila sasarannya adalah sistem elektronik di wilayah hukum Indonesia, sudah dapat

dikatakan melakukan tindak pidana dan dapat dihukum dengan hukum Indonesia.

Dilihat dari setiap pengaturan dalam bab perbuatan yang dilarang di UU ITE, materi yang diatur mirip dengan *Convention on Cybercrime* namun sistematikanya saja yang berbeda, yaitu:

1) Tindak pidana yang menggunakan sarana sistem komputer/ elektronik (Pasal 27-Pasal 29)
2) Tindak pidana terhadap sistem komputer/elektronik (Pasal 30-Pasal 35)

PENUTUP

Pengaturan dalam UU ITE dan Perubahannya mengadopsi ketentuan dalam *Convention on Cybercrime* dengan penyesuaian kontekstualisasi kebutuhan di Republik Indonesia. Pengaturan materi perbuatan yang dilarang juga mirip, yaitu *content-related offense* dan *offense toward electronic system*, namun menggunakan sistematika yang berbeda.

Kedepannya perlu ada penelitian yang membedah setiap unsur perbuatan yang dilarang agar dapat mengevaluasi kontekstualisasi kebutuhan pelarangan perbuatan di Indonesia, mengingat deklarasi UU ITE yang ingin menjadi rezim hukum siber.

DAFTAR BACAAN

BUKU

Balkin, Jack M. et al., *Cybercrime: Digital Cops in a Networked Environment*, New York University Press: New York, 2007

Bemmelen, J. M. van, *Hukum Pidana 3: Bagian khusus delik-delik khusus*, Binacipta: Bandung, 1986

Britz, Marjie T., *Computer Forensics and Cyber Crime: An Introduction*, Third Edition, Pearson Education Inc.: New Jersey, 2013

Golose, Petrus R., *Seputar Kejahatan Hacking: Teori dan Studi Kasus*, Yayasan Pengembangan Kajian Ilmu Kepolisian: Jakarta, 2008

Lamintang, P.A.F. dan Fransiscus J., *Dasar-dasar Hukum Pidana Indonesia*, Sinar Grafika: Jakarta, 2014

Lamintang, P.A.F. dan Djisman S., *Hukum Pidana Indonesia*, Sinar Baru: Bandung, 1990

Makarim, Edmon, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, Raja Grafindo Persada: Jakarta, 2005

McLuhan, Marshall, *Understanding Media*, Gingko Press: California, 2003

Soesilo, R., *Kitab Undang-undang Hukum Pidana Serta Komentar-komentarnya Lengkap Pasal Demi Pasal*, Politeia: Bogor,1996

Suseno, Sigid, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama: Bandung, 2012

Tresna, R., *Azas-azas Hukum Pidana*, Pustaka Tinta Mas: Bandung, 1994

Utrecht, E., *Hukum Pidana 1*, Pustaka Tinta Mas: Bandung, 1986

JURNAL

Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, Virginia Journal of Law and Technology, Vol. 9 No. 13, University of Virginia, 2004

Alamat Sekretariat **ARGUMENTUM**:
Program Studi Magister Ilmu Hukum
Fakultas Hukum Universitas Surabaya
Jalan Raya Kalirungkut, Surabaya 60293
T: 031-2981223;1225
F: 031-2981121
E: hukum@ubaya.ac.id atau wisnu@staff.ubaya.ac.id

9 772528 458007