BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan tentang Tindak Pidana, Pertanggungjawaban Pidana, dan Pemidanaan dalam Tindak Pidana *Cyber* dalam Convention on Cybercrime

Di poin A, penulis akan menguraikan isi dari perbuatan pidana yang diatur oleh CoC. CoC pada dasarnya tidak mengatur apa yang disebut tindak pidana, pertanggungjawaban pidana dan pemidanaan *cybercrime*. CoC mengembalikan rincian tindak pidana, pertanggungjawaban pidana dan pemidanaan *cybercrime* kepada hukum nasional. CoC memberikan acuan kepada hukum nasional untuk menentukan sendiri definisi perbuatan pidana, pertanggungjawaban pidana, dan pemidanaannya.

1. (Teks asli)

   Article 2 – Illegal access

   Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be 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.

(Terjemahan Pasal 2 – Akses Ilegal)

Masing-masing pihak harus mengambil tindakan legislatif dan tindakan lainnya yang mungkin diperlukan untuk ditetapkan sebagai tindak pidana dalam hukum nasionalnya, apabila perbuatan tersebut dilakukan dengan sengaja dan tanpa hak mengakses seluruh atau sebagian dari sistem komputer dengan tujuan untuk mendapatkan data komputer atau tujuan tidak jujur lainnya, atau sistem komputer yang berhubungan dengan sistem komputer lain.

2. *Article 3 – Illegal interception*

   Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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 computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

(Terjemahan Pasal 3 – Intersepsi ilegal)

Setiap pihak wajib mengambil tindakan legislatif dan tindakan lain yang diperlukan untuk ditetapkan sebagai sebagai tindak pidana di bawah hukum nasionalnya, ketika perbuatan tersebut dilakukan secara sengaja, penyadapan tanpa hak, dilakukan dengan maksud teknikal, transmisi data komputer ke, dari atau ke dalam suatu sistem komputer, termasuk gelombang elektromagnetik dari suatu sistem komputer yang membawa data komputer. Pihak tersebut dapat menuntut bahwa tindakan tersebut dilakukan dengan niat tidak jujur, atau berhubungan dengan sistem komputer yang terhubung dengan komputer sistem lain.

3. *Article 4 – Data Interference*

   (a) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

   (b) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

   (Terjemahan Pasal 4 – Gangguan data)

   (a) Masing-masing Pihak harus mengambil tindakan legislatif dan tindakan lainnya yang mungkin diperlukan untuk

ditetapkan sebagai tindak pidana dalam hukum nasionalnya, ketika perbuatan tersebut dilakukan tanpa hak dengan sengaja, sehingga terdapat kerusakan, penghapusan, kemunduran, perubahan atau penindasan data di komputer.

(b) Masing-masing pihak dapat mencadangkan hak memaksa apabila tindak pidana seperti yang disebutkan dalam paragraph 1 menyebabkan kerusakan yang parah.

4. *Article 5 – System interference*

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

(Terjemahan Pasal 5 – Gangguan sistem)

Masing-masing pihak harus mengambil tindakan legislatif dan tindakan lainnya yang mungkin diperlukan untuk ditetapkan sebagai tindak pidana dalam hukum nasionalnya, apabila dilakukan dengan sengaja, penghalangan serius tanpa hak untuk mengfungsikan suatu sistem komputer dengan memasukkan, mengirimkan, merusak, menghapus, menurunkan fungsi, mengubah atau menindas suatu data komputer.

Pasal 2, 3, 4 dan 5 adalah pasal yang saling berhubungan satu sama lain. Pasal 2 merupakan awal dari terjadinya *cybercrime*, yaitu dengan adanya akses ilegal yang dilakukan oleh pelaku. Pasal 3, 4 dan 5 merupakan akibat lanjutan dari pasal 2, yaitu terjadinya kerusakan sistem, kerusakan data, penyadapan dalam sistem komputer. Pelaku yang melakukan akses ilegal terhadap suatu sistem komputer yang menyebabkan kerusakan sistem, dapat dikenakan pasal berlapis dari hukum nasional negara yang meratifikasi.

Cybercrime dapat diartikan sebagai kejahatan dua arah, *crime against computer* dan *crime using computer*. *Crime against computer* artinya tindak pidana yang dilakukan kepada komputer, sebagai contoh akses ilegal yang dilanjutkan dengan penyerangan sistem menggunakan virus. Yang baru saja terjadi adalah virus *WannaCry*, yang menyerang sistem komputer di sejumlah negara. Selanjutnya, *crime using computer*. Pelaku penyebar virus *WannaCry* selain melakukan tindak pidana yang menyerang sistem komputer juga melakukan tindak pidana menggunakan komputer. Pelaku menggunakan virus komputer untuk membajak sistem komputer dan mengakibatkan hilang atau terkuncinya data-data dalam komputer tersebut. Pelaku kemudian meminta tebusan kepada pemilik komputer, namun tanpa adanya jaminan bahwa data komputer tersebut akan kembali seperti semula.

5. *Article 6 – Misuse of devices*

   (a) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(1) 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 any of the offences established in Articles 2 through 5; and

(2) The possession 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.

(b) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 if this article is not for the purpose of committing an offence established in accordance with Article 2 through 5 of this Convention,

such as for the authorised testing or protection of a computer system.

(c) Each party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

(Terjemahan Pasal 6 – Penyalahgunaan alat-alat yang berhubungan dengan komputer)

(a) Masing-masing pihak harus mengambil tindakan legislatif dan tindakan lainnya yang mungkin diperlukan untuk ditetapkan sebagai tindak pidana dalam hukum nasionalnya, apabila dilakukan dengan sengaja dan tanpa hak:

(b) Produksi, penjualan, pengadaan untuk penggunaan, impor, distribusi atau kegiatan lainnya sehingga tersedianya:

i. Suatu alat, termasuk program komputer, yang didesain atau diadaptasi terutama untuk tujuan melakukan tindak pidana seperti yang disebutkan dalam pasal 2 hingga pasal 5;

ii. Kata sandi komputer, kode akses, atau data yang serupa sehingga menyebabkan seluruh atau sebagian sistem komputer dapat diakses,

Dengan tujuan bahwa yang disebut di atas digunakan untuk melakukan tindakan pidana sesuai yang ditetapkan dalam pasal 2 sampai dengan pasal 5; dan

(c) Kepemilikan sebuah benda seperti yang disebutkan dalam poin i dan ii di atas, dengan tujuan untuk digunakan sebagai tindak pidana sesuai yang ditetapkan dalam pasal 2 sampai dengan 5 konvensi ini, seperti untuk pengujian atau perlindungan resmi dari sistem komputer.

(d) Setiap Pihak berhak untuk tidak menerapkan ayat 1 pasal ini, dengan ketentuan bahwa reservasi tersebut tidak menyangkut penjualan, distribusi, atau penyediaan barang-barang sebagaimana dimaksud dalam ayat 1 a.ii dari pasal ini.

Dalam ayat (1) huruf (a), alat yang dimaksud merupakan *software* komputer untuk melakukan penyadapan, pengrusakan sistem, data, dan lain-lain. Di beberapa hukum nasional *software* ini lebih mengarah kepada virus komputer yang menyerang sistem. Seperti yang baru-baru ini terjadi, yaitu virus *ransomware "Wannacry"* yang menyerang sejumlah sistem komputer di berbagai negara di dunia.

6. *Article 7 – Computer-related forgery*

   Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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 legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

(Terjemahan Pasal 7 – Pemalsuan di Komputer)

Setiap pihak harus mengambil tindakan legislatif dan tindakan lainnya yang diperlukan untuk ditetapkan sebagai tindak pidana, ketika dilakukan dengan sengaja dan tanpa hak, memasukkan, pengubahan, penghapusan, atau penekanan data komputer, menyebabkan data yang tidak otentik dengan tujuan untuk digunakan seolah-olah data tersebut adalah data otentik, tanpa peduli apakah data tersebut dapat dibaca secara langsung dan jelas. Pihak tersebut mungkin memiliki niat untuk menipu, atau tujuan tidak jujur lainnya, sebelum tanggung jawab pidananya menempel.

7. *Article 8 – Computer-related fraud*

   Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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.

(Terjemahan Pasal 8 – Penipuan dengan komputer)

Masing-masing pihak wajib mengambil tindakan legislative dan tindakan lainnya yang mungkin diperlukan untuk menetapkan tindak pidana dalam hukum nasionalnya, ketika perbuatan tersebut dilakukan dengan tujuan dan tanpa hak, menyebabkan kehilangan kepemilikan seseorang dengan:

(a) Memasukkan sesuatu, pengubahan, atau penekanan data komputer;

(b) Gangguan lain dalam fungsi sistem komputer,

Dengan tujuan curang atau tidak jujur untuk mendapatkan keuntungan ekonomi tanpa hak untuk perseorangan atau untuk orang lain.

Pasal 7 dan pasal 8 merupakan pasal tindakan pidana umum seperti tindak pidana yang dilakukan secara langsung di dunia nyata, yaitu pencurian, penipuan, untuk mendapatkan suatu keuntungan ekonomi bagi pelakunya. Di beberapa negara sudah terdapat perkembangan tindak pidana umum yang dilakukan secara *online* ini, yaitu korupsi *online*, membuat video yang dapat mempengaruhi penontonnya untuk bunuh diri

(walaupun hal ini agak sulit dibuktikan karena adanya kemungkinan pengaruh hipnotis terhadap pelaku bunuh diri). Yang paling umum terjadi adalah adanya telepon atau pesan pendek yang mengindikasikan bahwa korban harus mengirimkan sejumlah uang kepada orang yang menghubunginya.

8. *Article 9 – Offences related to child pornography*

(a) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

i. Producing child pornography for the purpose of its distribution through a computer system;

ii. Offering or making available child pornography through a computer system;

iii. Distributing or transmitting child pornography through a computer system;

iv. Procuring child pornography through a computer system for oneself or for another person;

v. Possessing child pornography in a computer system or on a computer-data storage medium.

(b) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

i. A minor engaged in sexually explicit conduct;

ii. A person appearing to be a minor engaged in sexually explicit conduct;

iii. Realistic images representing a minor engaged I sexually explicit conduct.

(c) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(d) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

(Terjemahan Pasal 9 - Tindak Pidana Pornografi Anak-anak)

(a) Masing-masing pihak harus mengambil tindakan legislatif dan tindakan lain yang diperlukan untuk menetapkan tindak pidana dalam hukum nasionalnya, jika perbuatan ini dilakukan dengan sengaja dan tanpa hak, sebagai berikut:

i. Memproduksi pornografi anak dengan tujuan mendistribusikan melalui suatu sistem komputer;

ii. Menawarkan atau menyediakan pornografi anak melalui suatu sistem komputer;

iii. Mendistribusikan atau mentransmisikan pornografi anak melalui suatu sistem komputer;

iv. Mendapatkan pornografi anak melalui sistem komputer untuk dirinya sendiri atau untuk orang lain;

v. Memiliki pornografi anak dalam sistem komputernya atau sebagai data komputer di penyimpanannya.'

(b) Yang dimaksud dalam paragraf 1 di atas, istilah "pornografi anak" harus berisi materi pornografi yang menggambarkan secara visual:

i. Anak yang terlibat dalam perilaku seksual eksplisit;

ii. Orang yang muncul dalam perilaku seksual eksplisit anak;

iii. Gambar realistic yang menunjukkan anak terlibat dalam perilaku seksual eksplisit.

(c) Istilah "anak" yang dimaksud dalam paragraf 2 artinya adalah semua orang yang berusia kurang dari 18 tahun. Masing-masing Pihak diperbolehkan untuk menentukan sendiri batas usianya, namun tidak diperbolehkan kurang dari 16 tahun.

(d) Masing-masing pihak diperbolehkan untuk tidak mencantumkan sebagian atau keseluruhan paragraf 1, sub-paragraf d. dan e., dan paragraf 2, sub-paragraf b. dan c.

Pornografi seksual anak belakangan ini sudah cukup berkembang pesat, dapat dibuktikan dengan adanya jual beli manusia yang bertujuan untuk digunakan sebagai budak atau pekerja seks komersial. Beberapa

negara semakin gencar melakukan penggalakan hukum terhadap pelaku pornografi anak ini, dan melakukan pencegahan dini terhadap pornografi seksual anak. Terhadap isu ini, negara-negara yang meratifikasi CoC sudah memiliki peraturan yang mencegah terjadinya pornografi dan tindak pornografi anak. Namun secara eksplisit pula, CoC tidak mengatur adanya tindak pornografi maupun pornografi seksual yang dilakukan oleh orang dewasa yang dianggap cakap hukum. CoC hanya mengatur tindakan yang dilarang terhadap pornografi anak. Pornografi anak diatur secara khusus dalam CoC karena terdapat beberapa konvensi awal yang memulai misalnya Deklarasi Universal Hak Asasi Manusia (DUHAM) dan *International Convention on Elimination of All Forms of Discrimation Againts Women* (CEDAW).

Dalam integrasi CoC ke dalam hukum nasional, hukum nasional dipengaruhi oleh budaya negara masing-masing. Indonesia yang merupakan negara berketuhanan, menjadikan norma kesusilaan dan norma agama juga termasuk di dalam hukum nasionalnya. Berbeda dengan Amerika Serikat dan Tiongkok; Amerika Serikat adalah negara liberal, dan Tiongkok adalah negara komunis. Walaupun di dua negara tersebut terdapat norma kesusilaan, namun kedudukan norma tersebut tidak dijunjung sekuat seperti di Indonesia. Oleh karena itu, peraturan di Amerika Serikat dan Tiongkok tidak mencantumkan pelanggaran kesusilaan bagi orang yang telah cakap hukum, namun hanya berfokus pada pornografi anak.

Di Amerika Serikat dan Tiongkok, walaupun norma kesusilaannya tidak dijunjung sekuat di Indonesia, namun perbedaan besar terletak pada persetujuan. Kegiatan seksual dan perbuatan lainnya merupakan tanggung jawab dari pelakunya masing-masing, terutama dalam hal persetujuan. Di Amerika Serikat dan Tiongkok, orang dewasa dianggap sudah tahu akan resiko dan konsekuensi yang terjadi jika melakukan perbuatan seksual (berbeda dengan pemerkosaan). Sedangkan di Indonesia kegiatan seksual sama sekali dilarang kecuali dilakukan dengan hubungan perkawinan, sesuai dengan norma kesusilaan dan keagamaan. Namun, baik di tiga negara tersebut melindungi anak dari pornografi dan kegiatan seksual, yang mana dirasa anak dianggap belum bisa memberi persetujuan terhadap kegiatan seksual tersebut.

B. Pengaturan tentang Tindak Pidana, Pertanggungjawaban Pidana, dan Pemidanaan dalam Tindak Pidana *Cyber* dalam United States Code § 18

U.S. Code adalah kitab undang-undang hukum pidana Amerika Serikat yang mengatur keseluruhan dari hukum yang ada. Negara-negara bagian pun menganut hukum berdasarkan U.S. Code, beserta dengan segala integrasi dan penambahan-penambahan seperlunya. Penulis menambahkan salah satu peraturan *cybercrime* di salah satu Negara bagian di Amerika Serikat, yaitu Michigan, yang akan diuraikan di bawah gambaran secara umum U.S. Code ini.

Cybercrime dalam US Code diatur dalam section 18. Terdapat 19 pasal yang mengatur tentang *cybercrime*, termasuk pasal pelanggaran hak cipta. Pasal-pasal tersebut secara keseluruhan sudah mengintegrasikan fungsi normatif dari CoC. Pasal-pasal ini tidak tersusun secara berurutan.

Berikut adalah uraian gambaran peraturan *cybercrime* dalam U.S. Code section 18 secara umum.

1. 18 U.S.C § 1028 – *Fraud and related activity in connection with identification documents, authentication features, and information.*

   Dalam pasal ini, diuraikan tentang tinda pidana penipuan dan tindak pidana lainnya yang berhubungan dengan pemalsuan dan penipuan dokumen-dokumen identifikasi, fitur otentikasi dan informasi. Seperti dalam KUHP Indonesia, terdapat perbuatan-perbuatan yang dilarang, yaitu memiliki, membuat, memiliki alat untuk membuat, menyimpan, memiliki dengan niat yang tidak baik, mengirimkan, menggunakan, atau menukarkan dengan sengaja dan tanpa hak. Hukuman untuk tindak pidana yang ada di pasal ini adalah hukuman penjara dari waktu 5 tahun sampai dengan 30 tahun penjara. Percobaan perbuatan pidana dihukum dengan hukuman yang sama dengan perbuatan yang telah dilakukan.

2. 18 U.S.C. § 1028a – *Aggravated identity theft.*

   Siapapun dilarang untuk menggunakan, mengirimkan, memiliki, tanpa hak yang sah, identifikasi atau dokumen palsu. Bagi yang melanggar akan dihukum penjara 2 sampai dengan 5 tahun. Dalam poin (b), pengadilan tidak diperbolehkan memberikan masa percobaan kepada orang yang melakukan pelanggaran pasal ini.

3. 18 U.S.C. § 1029 – *Fraud and related activity in connection with access devices.*

   Pasal ini menguraikan tentang perbuatan pembajakan komputer, baik komputer milik pemerintah Amerika Serikat mau pun komputer milik warga. Hukuman yang diberikan adalah hukuman penjara mulai dari 5 sampai dengan 20 tahun. Percobaan tindak pidana dihukum dengan hukuman penjara dari 5 sampai 10 tahun.

4. 18 U.S.C. § 1030 – *Fraud and related activity in connection with computers.*

   Pasal ini menguraikan tentang perbuatan pembajakan komputer, baik komputer milik Amerika Serikat mau pun komputer milik warga. Hukuman yang diberikan adalah hukuman penjara mulai dari 5 sampai

dengan 20 tahun. Percobaan tindak pidana dihukum dengan hukuman penjara dari 5 sampai dengan 10 tahun.

5. 18 U.S.C. § 1037 – *Fraud and related activity in connection with electronic mail*

   Secara umum, pasal ini menguraikan tentang ilegalnya pengiriman email dari komputer yang telah dibajak, perbuatan memalsukan kop surat elektronik, menggunakan informasi palsu saat mengakses surat elektronik. Pelanggaran akan pasal ini dihukum dengan hukuman penjara tidak lebih dari 3 sampai 5 tahun.

6. 18 U.S.C. § 1043 – *Fraud by wire, radio, or television.*

   Barangsiapa yang menggunakan televisi, radio, dan kabel dengan mengirimkan tulisan, tanda, sinyal, gambar atau suara dengan tujuan menguntungkan diri sendiri dengan cara menipu, dihukum penjara tidak lebih dari 20 tahun. Jika pelanggaran pasal ini menyebabkan kerugian pada institusi keuangan, maka pelakunya akan dikenai denda sebesar $1.000.000 dan/atau hukuman penjara tidak lebih dari 30 tahun.

7. 18 U.S.C. § 1466A, 2251, dan 2252, *child pornography*.

   3 pasal ini secara umum mengatur tentang perbatan pornografi seksual terhadap anak. Pasal 1466A mengatur tentang dilarangnya pendistribusian, kepemilikan,

penerimaan segala bentuk gambar, kartun, patung yang berbentuk atau melibatkan tubuh anak. Pasal 2251 melarang tentang pornografi seksual terhadap anak. Dalam pasal 2251 diuraikan pula pelanggaran maupun percobaan pelanggaran terhadap pasal tersebut dan beberapa pasal yang sesuai dengan pasal ini, dihukum paling sedikit 30 tahun sampai dengan 35 tahun, atau hukuman seumur hidup. Pasal 2252 mengatur tentang perbuatan pornografi seksual anak yang terdapat dalam video, gambar, buku, majalah, film, atau materi lain yang mengandung gambar bergerak. Percobaan pelanggaran dan pelanggaran perbuatan ini dihukum paling sedikit 5 tahun dan paling lama 40 tahun.

C. Pengaturan tentang Tindak Pidana, Pertanggungjawaban Pidana, dan Pemidanaan dalam Tindak Pidana *Cyber* dalam *Michigan Compiled Law*

Amerika Serikat memiliki 50 negara bagian. Negara bagian ini masing-masing memiliki hukum legislatifnya, yang merupakan turunan dari United States Code, yaitu hukum konstitusi umum Amerika Serikat. Dalam poin B ini, selain menguraikan *US Cyber Law* yang terdapat dalam *United States Code*, penulis juga akan menguraikan salah satu hukum *cyber* yang terdapat di salah satu

negara bagian Amerika Serikat, yaitu Michigan. Penulis memilih negara bagian Michigan dengan sumber hukum *Michigan Compiled Law* (selanjutnya disebut sebagai MCL), yang mana penulis anggap paling lengkap dan relevan, berdasarkan CoC dan *US Code***.**

Peraturan tentang *cybercrime* terdapat chapter 752, Act 53 of 1979 statute "*Fraudulent Access to Computers, Computer Systems, and Computer Networks*", *section* 752.791 - 752.797.

Sesuai dengan CoC dan *US Code Law*, peraturan tentang *cybercrime* yang terdapat di MCL sudah merupakan integrasi dari CoC dan *US Code Law*. Dalam Act 752 ini juga sudah diatur tentang tindak pornografi anak, dan secara khusus diatur dalam act 241 of 2004, statute "*Michigan Children's Protection Registry Act* (752.1061 - 752.1068)"

1. *Section 752.794 Prohibited access to computer program, computer, computer system, or computer network.*

   Sec. 4.

   A person shall not intentionally access or cause access to be made to a computer program, computer, computer system, or computer network to devise or execute a scheme or artifice with the intent to defraud or to obtain money, property, or a service by a false or fraudulent pretense, representation, or promise.

(Terjemahan Bagian 752.794 Larangan akses ke program komputer, komputer, sistem komputer, atau jaringan komputer.)

Bag. 4.

Seseorang dilarang mengakses atau membuka suatu akses secara sengaja untuk masuk ke dalam suatu program komputer, komputer, sistem komputer, atau jaringan komputer untuk merancang atau menjalankan sebuah skeman atau berbuat licik dengan tujuan untuk menipu untuk mendapatkan uang, benda-benda kepemilikan, atau pelayanan dengan kepura-puraan yang curang, perwakilan, atau kesepakatan.

2. *Section 752.795 Prohibited conduct.*

   Sec. 5.

   A Person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:

   a. *Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.'*

   b. *Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or*

attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network. This subdivision does not prohibit conduct protected under section 5 of article I of the state constitution of 1963 or under the first amendment of the constitution of the United States.

(Terjemahan Bagian 752. 795 perbuatan terlarang.)

Bag. 5.

Seseorang dilarang tanpa sengaja dan tanpa hak atau melebihi hak sahnya melakukan yang ada di bawah ini:

a. Mengakses atau membuat akses ke program komputer, komputer, sistem komputer, atau jaringan komputer untuk memperoleh, mengubah, merusak, menghapus, atau menghancurkan harta benda atau kegunaan lain atau jika tidak menggunakan pelayanan suatu program komputer, komputer, sistem komputer, atau jaringan komputer.
b. Memasukkan atau menempelkan atau dengan sadar membuat kesempatan masuknya atau menempelnya

instruksi yang tidak diketahui dan tidak diinginkan pada program komputer, komputer, sistem komputer, atau jaringan komputer, yang dimaksudkan untuk memperoleh, mengubah, merusak, menghapus, mengganggu atau menghancurkan harta benda atau menggunakan fungsi program komputer, komputer, sistem komputer, atau jaringan komputer. Subbagian ini tidak melarang tindakan yang dilindungi di bawah bagian 5 Pasal I konstitusi Negara bagian tahun 1963 atau di bawah amandemen pertama konstitusi Amerika Serikat.

Pasal ini merupakan pasal yang melarang perbuatan akses ilegal yang menyebabkan berubahnya data komputer yang terdapat di dalam komputer yang diakses. Namun terdapat pengecualian terhadap pasal ini, yaitu bagian 5 pasal I Konstitusi Negara Bagian Michigan tahun 1963. Pasal tersebut berbunyi: "Setiap orang dapat bicara, menulis, mengekspresikan dan mempublikasikan secara bebas pandangannya terhadap segala sesuatu, bertanggung jawab terhadap penyalahgunaan hak tersebut; dan tidak ada hukum yang akan diberlakukan untuk menahan atau menghilangkan kebebasan berbicara atau pers." Artinya warga diperbolehkan mengekspresikan pendapatnya dengan bebas, dengan cara apa pun, yang juga berarti bahwa perbuatan akses illegal yang dilakukan

untuk mengekpresikan pendapatnya dilindungi dan tidak dikenai hukuman.

3. *Section 752.795a Michigan children's protection registry act; violation.*

   Sec. 5a.

   A violation of the Michigan children's protection registry act is a violation of this act.

   Pelanggaran terhadap *Michigan children's protection registry act* dianggap melakukan pelanggaran terhadap pasal ini.

Dalam pasal ini, terdapat satu bagian khusus yang mengatur tentang tindak pidana *cyber* yang dilakukan oleh/kepada anak. Hukumannya diatur pada pasal 752.795a, 752.796a dan 752.796b. Rincian peraturan yang terdapat dalam *Michigan children's protection registry act* adalah sebagai berikut:

a. *Section 752.1065 Prohibited conduct; exceptions; third-party security audits.*

   Sec. 5.

   (1) Except as otherwise provided under this section, a person shall not send, cause to be sent, or conspire with a third party to send a message to a contact point that has been registered for more than 30 calendar days with the department if the primary purpose of the

message is to, directly or indirectly, advertise or otherwise link to a message that advertises product or service that a minor is prohibited by law from purchasing, viewing, possessing, participating in, or otherwise receiving.

(2) *A person desiring to send message described in subsection (1) shall use the mechanism created under section 3(6) to ensure compliance with this act.*

(3) *The consent of a minor or third party to receive the message is not a defense to a violation of this action.*

(4) *A person does not violate this act because the person is an intermediary between the sender and recipient in the transmission of an electronic message that violates this act or unknowingly provides transmission of electronic messages over the person's computer network or facilities that violate this act.*

(5) *The sending of a message described in subsection (1) is prohibited only if it is otherwise a crime for the minor to purchase, view, possess, participate in, or otherwise receive the product or service.*

(6) *The sending of a message described in subsection (1) is not prohibited if prior to sending the message the sender has obtained from an age-verified adult an*

affirmative statement of consent to receive the message at an adult designated contact point. To comply with this subsection, the sender shall do all of the following:

(a) Verify that the person making the affirmative statement is of legal age by inspecting in a face to face transaction a valid government-issued photo identification with proof of age.

(b) Obtain a written record stating that the recipient has consented to receive the type of messages described in subsection (1). The consent form require under this subdivision shall be signed by the recipient. The sender shall retain the consent form required under this subdivision and make it available for verification as may be required under subdivision (d).

(c) All messages allowed under this subsection shall include notice to the recipient that he or she may rescind their consent and provide an opportunity for the recipient to opt out of receiving any future messages.

(d) Notify the department that the sender intends to send messages as allowed under this subsection. The department may implement procedures to

verify that the sender is in compliance with this subsection.

(7) Within 90 days of the effective date of the amendatory act that added this subsection, the department, or the vendor providing registry services for the department, shall conduct a third-party audit to certify the security of the registry. Follow up third-party security on the registry systems shall be conducted at least annually. If the third-party security audit determines that the registry does not meet or exceed the industry standard for high security systems, then the registry shall be suspended until the security systems are determined to meet this standard.

(Terjemahan Pasal 752.1065 Perbuatan yang dilarang; pengecualian; audit keamanan pihak ketiga.)

Bag. 5.

(1) Kecuali sebaliknya telah disebutkan di pasal di bawah ini, seseorang tidak diperbolehkan mengirim, menyebabkan dikirim, atau berkonspirasi dengan pihak ketiga untuk mengirim pesan ke kontak yang sudah didaftarkan dalam waktu lebih dari 30 hari kalender dengan departemen jika tujuan utama dari pesan tersebut adalah untuk, secara langsung atau tidak langsung, mengiklankan atau menautkan ke sebuah

pesan yang mengiklankan produk atau layanan yang dilarang oleh undang-undang dari pembelian, penyajian, kepemilikan, partisipasi, atau penerimaan.

(2) Seseorang yang ingin mengirimkan pesan seperti yang dideskripsikan dalam subbagian (1) wajib dikenakan mekanisme yang dibuat di bawah pasal 3(6) untuk memastikan pemenuhan pasal ini.

(3) Persetujuan anak atau pihak ketiga yang menerima pesan bukan merupakan pembelaan dari pelanggaran pasal ini.

(4) Seseorang tidak melanggar pasal ini karena seseorang merupakan perantara pengirim dan penerima dalam transmisi pesan elektronik yang melanggar pasal ini atau secara tidak diketahui menyediakan transmisi pesan elektronik melalui komputer orang lain atau fasilitas lain yang melanggar pasal ini.

(5) Pengiriman pesan yang dideskripsikan pada subbagian (1) dilarang hanya jika sebaliknya, sebuah kejahatan bagi anak untuk membeli, melihat, memiliki, berpartisipasi, atau menerima produk atau layanan tersebut.

(6) Pengiriman pesan seperti yang dideskripsikan di subbagian (1) dilarang jika sebelum mengirim pesan yang telah diperoleh pengirim dari orang dewasa yang diverifikasi usia sebuah pernyataan persetujuan untuk menerima pesan tersebut pada

titik kontak yang ditunjuk orang dewasa. Untuk memenuhi subbagian ini, pengirim harus telah melakukan hal di bawah ini:

(a) Memeriksa bahwa orang yang membuat pernyataan pembenaran telah berusia cukup secara hukum dengan menginspeksi transaksi tatap muka identifikasi foto yang dikeluarkan oleh pemerintah dengan bukti usia.

(b) Mendapatkan rekaman tertulis yang menyatakan bahwa penerima telah menyetujui untuk menerima tipe pesan yang dijelaskan dalam subbagian (1). Blanko persetujuan ayng didapatkan dari subdivisi ini harus ditandatangani oleh penerima. Pengirim wajib menyimpan blangko persetujuan yang diperlukan di bawah subbagian ini dan menyiapkannya untuk verifikasi yang diperlukan di bawah subbagian (d).

(c) Semua pesan-pesan yang diperbolehkan di bawah subbagian ini wajib memasukkan peringatan ke pengirim bahwa dia dapat membatalkan persetujuannya dan memberi kesempatan kepada pengirim memilih untuk tidak menerima pesan di masa mendatang.

(d) Memberi tahu pihak yang mana pengirim berniat untuk mengirim pesan yang diperbolehkan dalam subbagian ini. Pihak tersebut dapat mengimplementasikan prosedur

untuk memverifikasi bahwa pengirim memenuhi unsur subbagian in

(7) Dalam waktu 90 hari setelah tanggal berlakunya pasal yang telah diamandemen dan ditambahkan ke dalam subbagian ini, pihak, atau vendor yang menyediakan layanan registrasi untuk departemen, wajib melakukan audit keamanan pihak ketiga untuk mensertifikasi keamanan registri. Tindak lanjut audit keamanan pihak ketiga pada sistem registri harus dilakukan setidaknya setiap tahun. Jika audit keamanan pihak ketiga bahwa registri tidak memenuhi atau tidak melampaui standar industri untuk sistem keamanan yang tinggi, maka registri wajib ditangguhkan sampai dengan sistem keamanannya dipastikan dapat memenuhi standar yang ditentukan.

Dalam pasal ini diatur secara ketat bahwa anak dilarang menerima, melakukan, mengirim, melihat pesan-pesan yang isinya dilarang oleh undang-undang. Pasal ini mengatur perlindungan anak dengan cukup ketat. Apabila terdapat pengiriman pesan yang berisi mengiklankan atau menautkan ke sebuah pesan yang mengiklankan produk atau layanan yang dilarang oleh undang-undang dari pembelian, penyajian, kepemilikan, partisipasi, atau penerimaan, maka penerima harus mendapat persetujuan terlebih dahulu, terkait dengan usia, apakah orang tersebut cukup umur dan cakap hukum.

4. *Section 752.796 Use of computer program, computer system, or computer network to commit crime.*

   Sec 6.

   (1) A person shall not use a computer program, computer, computer system, or computer network to commit, attempt to commit, conspire to commit, or solicit another person to commit a crime.

   (2) This section does not prohibit a person from being charged with, convicted of, or punished for any other violation of law committed by that person while violating or attempting to violate tis section, including the underlying offense.

   (3) This section applies regardless of whether the person is convicted of committing, attempting to commit, conspiring to commit, or soliciting another person to commit the underlying offense.

(Terjemahan Bagian 752.796 penggunaan program komputer, sistem komputer, atau jaringan komputer untuk melakukan tindakan kriminal.)

Bag. 6.

(1) Seseorang dilarang menggunakan program komputer, sistem komputer, atau jaringan komputer untuk melakukan, mencoba

melakukan, bekerja sama melakukan, atau mengajak orang lain untuk melakukan tindak kriminal.

(2) Bagian ini tidak menghentikan orang dari dibebani, didakwa, atau dihukum karena pelanggaran hukum yang dilakukan oleh orang lain saat melanggar atau mencoba melanggar bagian ini, termasuk dengan pelanggaran yang mendasar.

(3) Bagian ini diterapkan tanpa peduli apakah orang tersebut didakwa melakukan, mencoba melakukan, bekerja sama melakukan, atau mengajak orang lain melakukan degan pelanggaran yang mendasar.

Perbuatan kriminal yang dimaksud dalam pasal ini adalah perbuatan kriminal secara umum. Pencurian, penipuan, korupsi, dan lain-lain. Perbuatan ini dilakukan dengan menggunakan program komputer, yang juga dapat berupa virus. Salah satu contohnya, virus komputer yang menyerang ke sejumlah sistem komputer. Kemudian si pembuat virus akan meminta jaminan untuk dikembalikannya sistem komputer seperti semua dengan sejumlah bayaran, namun tetap saja tidak ada jaminan bahwa setelah sejumlah uang dibayarkan sistem komputer akan kembali seperti semula.

5. *Section 752.796a Violation of MCL 752.795a; penalties, exception; defense; burden proof; effective date of section. Sec. 6a.*

(1) A person who violates section 5a is guilty of the following:

(a) For the first violation, a misdemeanor punishable by imprisonment for not more than 1 year or a fine not more than $10,000.00, or both.

(b) For the second violation, a felony punishable by imprisonment for not more than 2 year or a fine of not more than $20,000.00, or both.

(c) For the third and any subsequent violation, a felony punishable by imprisonment for not more than 3 years or a fine of not more than $30,000.00, or both.

(2) A person does not violate section 5a because the person is intermediary between the sender and recipient in the transmission of an electronic message that violates section 5a or unknowingly provides transmission of electronic messages over the person's computer network or facilities that violate section 5a.

(3) It is a defense to an action brought under this section that the communication was transmitted accidentally. The burden of proving that the communication was transmitted accidentally is on the sender.

(4) This section does not take effect until July 1, 2005.

(Terjemahan Bagian 752.796a Pelanggaran MCL 752.795a; Hukuman, pengecualian, pembelaan, beban pembuktian, tanggal efektif pelaksanaan pasal.

Sec. 6a

(1) Seseorang yang melanggar bagian 5a dinyatakan bersalah karena berikut ini:

(a) Pelanggaran pertama, dianggap kejahatan ringan yang harus dihukum dengan hukuman penjara tidak lebih dari 1 tahun atau denda tidak lebih dari $10,000.00, atau keduanya.

(b) Pelanggaran kedua, dianggap kejahatan besar yang harus dihukum dengan hukuman penjara tidak lebih dari 2 tahun atau denda tidak lebih dari $20,000.00, atau keduanya.

(c) Pelanggaran ketiga atau seterusnya, dianggap kejahatan besar yang harus dihukum dengan hukuman penjara tidak lebih dari 3 tahun atau denda $30,000.00, atau keduanya.

(2) Seseorang tidak melanggar bagian 5a karena orang tersebut adalah penghubung antara pengirim dan penerima dalam pengiriman pesan elektronik yang melanggar bagian 5a atau secara tidak sadar membantu pengiriman pesan elektronik ke jaringan komputer orang lain atau fasilitas yang melanggar bagian 5a.

(3) Ini adalah pembelaan terhadap tindakan yang dilakukan di bawah bagian ini bahwa komunikasi tersebut ditransmisikan secara tidak

sengaja. Pembuktian bahwa komunikasi yang ditransmisikan secara tidak sengaja dibebankan kepada pengirim.

6. *Section 752.796b Money, income and property subject to seizure and forfeiture.*

   Sec. 6b.

   All money and other income, including all proceeds earned but not yet received by a defendant from a third party as a result of the defendant's violations of this act, and all computer equipment, all computer software, and all personal property used in connection with any violation of this act known by the owner to have been used in violation of this act are subject to lawful seizure and forfeiture in the same manner as provided under sections 4701 to 4709 of the revised judicature act of 1961, 1961 PA 236, MCL 600.4701 to 600.4709.

(Terjemahan Bagian 752.796b Uang, pemasukan dan harta beda tunduk pada perampasan dan penyitaan.)

Bag. 6b.

Semua uang dan pemasukan lain, termasuk yang didapatkan dalam proses namun belum didapatkan oleh terdakwa dari pihak ketiga atas hasil pelanggaran terdakwa terhadap pasal ini, dan semua peralatan komputer, semua perangkat lunak komputer, dan semua harta benda pribadi yang digunakan berhubungan dengan

pelanggaran pasal ini, yang diketahui oleh pemilik bahwa telah digunakan untuk melakukan pelanggaran terhadap pasal ini, tunduk pada perampasan dan penyitaan secara hukum dengan cara yang sama seperti yang sudah terdapat dalam bagian 4701 sampai dengan 4709 yang telah direvisi dengan peraturan hakim tahun 1961, 1961 PA 26, MCL 600.4701 sampai dengan 600.4709.

7. *Section 752.797 Penalties; prior convictions; presumption; reimbursement order; definition.*

   Sec. 7.

   (1) A person who violates section 4 is guilty of a crime as follows:

   (a) If the violation involves an aggregate amount of less than $200.00, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $500.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine.

   (b) If any of the following apply, the person is guilty of a misdemeanor punishable by imprisonment for not more than 1 year or a fine of not more than $2000.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of $200.00 or more but less than $1,000.00.

(ii) The person violates this act and has a prior conviction.

(c) If any of the following apply, the person is guilty of felony punishable by imprisonment for not more than 5 years or a fine of not more than $10,000.00 or 3 times the aggregate amount, whichever is greater, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of $1,000.00 or more but less than $20,000.00.

(ii) The person has 2 prior convictions.

(d) If any of the following apply, the person is guilty of a felony punishable by imprisonment for not more than 10 years or a fine of not more than 3 times the aggregate amount, or both imprisonment and a fine:

(i) The violation involves an aggregate amount of $20,000.00 or more.

(ii) The person has 3 or more prior convictions.

(2) A person who violates section 5 is guilty of a crime as follows:

(a) Except as provided in subdivision (b), the person is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than $10,000.00 or both.

(b) If the person has a prior conviction, the person is guilty of felony punishable by imprisonment for not more than 10 years or a fine of not more than $50,000.00, or both.

(3) A person who violates section 6 is guilty of a crime as follows:

(a) If the underlying crime is a misdemeanor or a felony with a maximum term of imprisonment of 1 year or less, the person is guilty of a misdemeanor punishable by imprisonment for not more than 1 year or a fine of not more than $5,000.00, or both.

(b) If the underlying crime is a misdemeanor or a felony with a maximum term of imprisonment of 1 year but less than 2 years, the person is guilty of a felony punishable by imprisonment for not more than 2 years or a fine or not more than $5,000.00, or both.

(c) If the underlying crime is a misdemeanor or a felony with a maximum term of imprisonment of 2

years or more but less than 4 years, the person is guilty of a felony punishable by imprisonment for not more than 4 years or a fine of not more than $5,000.00, or both.

(d) If the underlying crime is a felony with a maximum term of imprisonment of 4 years or more but less than 10 years, the person is guilty of a felony punishable by imprisonment for not more than 7 years or a fine of not more than $5,000.00, or both.

(e) If the underlying crime is a felony punishable by a maximum term of imprisonment of 10 years or more but less than 20 years, the person is guilty of a felony punishable by imprisonment for not than 10 years or a fine of not more than $10,000.00, or both.

(f) If the underlying crime is a felony punishable by a maximum term of imprisonment of 20 years or more or for life, the person is guilty of felony punishable by imprisonment for not more than 20 years or a fine of not more than $20,000.00, or both.

(4) The court may order that a term of imprisonment imposed under subsection (3) be served consecutively to

any term of imprisonment imposed for conviction of the underlying offense.

(5) If the prosecuting attorney intends to seek an enhanced sentence under section 4 or section 5 based upon the defendant having a prior conviction, the prosecuting attorney shall include on the complaint and information a statement listing that prior conviction. The existence of the defendant's prior conviction shall be determined by the court, without a jury, at sentencing. The existence of a prior conviction may be established by any evidence relevant for that purpose, including, but not limited to, 1 or more of the following:

(a) A copy of the judgment of conviction.

(b) A transcript of a prior trial, plea-taking, or sentencing.

(c) Information contained in a presentence report.

(d) The defendant's statement.

(6) It is a rebuttable presumption in a prosecution for a violation of section 5 that the person did not have authorization from the owner, system operator, or other person who has authority from the owner of system operator to grant permission to access the computer program, computer, computer system, or computer

network or has exceeded authorization unless 1 or more of the following circumstances existed at the time of access:

(a) Written or oral permission was granted by the owner, system operator, or other person who has authority from the owner of system operator to grant permission of the accessed computer program, computer, computer system, or computer network.

(b) The accessed computer program, computer, computer system, or computer network had a pre-programmed access procedure that would display a bulletin, command, or other message before access was achieved that a reasonable person would believe identified the computer program, computer, computer system, or computer network as within the public domain.

(c) Access was achieved without the use of a set of instructions, code, or computer program that bypasses, defrauds, or otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network.

(7) The court may order a person convicted of violating this act to reimburse this state or a local unit of government of this state for expenses incurred in relation to the violation in the same manner that expenses may be ordered to be reimbursed under section 1f of chapter IX of the code of criminal procedure, 1927 PA 175, MCL 769.1f.

(8) As used in this section, "prior conviction" means a violation or attempted violation of section 145d of the Michigan penal code, 1931 PA 328, MCL 750.145d, or this act or a substantially similar law of the United States, another state, or a political subdivision of another state.

(Terjemahan Bagian 752.797 Hukuman, dakwaan prioritas, anggapan, perintah pengembalian, ketentuan lain.)

Bag. 7.

(1) Seseorang yang melanggar pasal 4 dinyatakan bersalah melakukan tindak pidana sebagai berikut:

(a) Jika pelanggaran melibatkan jumlah yang apabila dikumpulkan mencapai kurang dari $200.00, orang tersebut dinyatakan bersalah akan tindak pidana ringan yang harus dihukum dengan hukum penjara tidak lebih dari 93 hari atau denda tidak lebih dari $500.00 atau 3 kali

dari jumlah yang diakumulasikan, yang mana lebih besar, atau hukum penjara dan denda.

(b) Jika hal berikut berlaku, seseorang yang bersalah atas tindak pidana ringan yang harus dihukum dengan hukum penjara tidak lebih dari 93 hari atau denda tidak lebih dari $500.00 atau 3 kali dari jumlah yang diakumulasikan, yang mana lebih besar, atau hukum penjara dan denda:

(i) Pelanggaran melibatkan total jumlah $200.00 atau lebih namun kurang dari $1,000.00.

(ii) Seseorang melanggar pasal ini dan sudah didakwa terlebih dahulu.

(c) Jika hal berikut berlaku, maka orang yang bersalah atas tindak pidana berat yang harus dihukum tidak lebih dari 5 tahun atau denda tidak lebih dari $10,000.00 atau 3 kali lebih besar dari jumlah total yang dikumpulkan, yang mana lebih besar, atau hukum penjara dan denda:

(i) Pelanggaran melibatkan jumlah keseluruhan sebesar $1,000.00 atau lebih namun kurang dari $20,000.00.

(ii) Orang tersebut sudah didakwa dengan 2 dakwaan.

(d) Jika hal berikut berlaku, maka orang yang bersalah atas tindak pidana berat harus dihukum tidak lebih dari 10 tahun atau denda 3 kali lebih besar dari jumlah total yang

dikumpulkan, yang mana lebih besar, atau hukum penjara dan denda:

(i) Pelanggaran tersebut melibatkan jumlah keseluruhan $20,000.00 atau lebih.

(ii) Orang tersebut sudah didakwa dengan 3 dakwaan.

(2) Seseorang yang melanggar pasal 5 dinyatakan bersalah melakukan tindak pidana sebagai berikut:

(a) Seperti pengecualian di subbagian (b), seseorang yang dinyatakan bersalah karena tindak pidana berat harus dihukum hukuman penjara tidak lebih dari 5 tahun atau denda tidak lebih dari $10,000.00, atau keduanya.

(b) Jika orang tersebut sudah didakwa dengan dakwaan lain sebelumnya, orang tersebut dinyatakan bersalah atas tindak pidana berat harus dihukum hukuman penjara tidak lebih dari 10 tahun dan denda tidak lebih dari $50,000.00, atau keduanya.

(3) Seseorang yang melanggar pasal 6 dinyatakan bersalah melakukan tindak pidana sebagai berikut:

(a) Jika tindak pidana yang mendasar adalah tindak pidana ringan atau tindak pidana berat dengan hukuman penjara maksumal 1 tahun atau kurang, orang yang bersalah atas tindak pidana ringan harus dihukum hukuman penjara tidak

lebih dari 1 tahun atau denda tidak lebih dari $5,000.00, atau kurang.

(b) Jika tindak pidana yang mendasar adalah tindak pidana ringan atau tindak pidana berat dengan hukuman penjara lebih dari 1 tahun namun kurang dari 2 tahun, maka orang tersebut dinyatakan bersalah atas tindak pidana berat yang harus dihukum hukuman penjara tidak lebih dari 2 tahun atau denda tidak lebih dari $5,000.00, atau keduanya.

(c) Jika tindak pidana yang mendasar adalah tindak pidana ringan atau tindak pidana berat dengan hukuman penjara 2 tahun atau lebih lebih namun kurang dari 4 tahun, orang tersebut dinyatakan bersalah atas tindak pidana berat yang harus dihukum hukum penjara tidak lebih dari 4 tahun atau denda tidak lebih dari $5,000.00, atau keduanya.

(d) Jika tindak pidana yang mendasari adalah tindak pidana berat dengan hukuman maksimal 4 tahun atau lebih namun kurang dari 10 tahun, orang tersebut dinyatakan bersalah atas tindak pidana berat yang harus dihukum hukum penjara tidak lebih dari 7 tahun atau denda tidak lebih dari $5,000.00, atau keduanya.

(e) Jika tindak pidana yang mendasari adalah tindak pidana berat dengan hukuman maksimal 10 tahun atau lebih namun kurang dari 20 tahun, orang tersebut dinyatakan

bersalah atas tindak pidana berat yang harus dihukum penjara tidak lebih dari 10 tahun atau denda tidak lebih dari $10,000.00, atau keduanya.

(f) Jika tindak pidana yang mendasari adalah tindak pidana berat yang harus dihukum dengan hukuman maksimal 20 tahun atau lebih atau seumur hidup, orang yang dinyatakan bersalah atas tindak pidana berat harus dihukum hukuman penjara tidak lebih dari 20 tahun atau denda tidak lebih dari $20,000.00, atau keduanya.

(4) Pengadilan dapat memerintahkan ketentuan hukuman penjara yang dikenakan di bawah subpasal (3) dilaksanakan berurutan dengan ketentuan hukuman penjara yang dikenakan untuk dakwaan yang telah mendasari tindak pidana.

(5) Jika jaksa penuntut berniat untuk mencari peningkatan hukuman dari pasal 4 dan pasal 5 berdasarkan terdakwa yang memiliki dakwaan sebelumnya, jaksa penuntut harus menyertakan keluhan dan informasi yang terdapat dalam dakwaan sebelumnya. Eksistensi dakwaan sebelumnya harus ditentukan oleh pengadilan, tanpa juri, saat penghukuman. Eksistensi dakwaan sebelumnya dapat ditetapkan oleh bukti apapun yang relevan untuk tujuan itu, termasuk, tetapi tidak terbatas pada, 1 atau lebih dari berikut ini:

(a) Salinan dari dakwaan penilaian.

(b) Transkrip pengadilan sebelumnya, permohonan peneguhan, hukuman.

(c) Informasi berkaitan laporan pra-hukuman.

(d) Pernyataan terdakwa.

(6) Pelanggaran pasal 5 dapat disanggah dengan asumsi dalam penuntutan bahwa seseorang tidak memiliki izin sah dari pemilik, operator sistem, atau orang lain yang memiliki hak dari pemilik atau operator sistem untuk memberikan izin untuk mengakses program komputer, komputer, sistem komputer, atau jaringan komputer atau telah melewati izin sah kecuali 1 atau lebih dari keadaan berikut ini yang terjadi dalam waktu akses:

(a) Izin tertulis atau lisan telah diberikan oleh pemilik, operator sistem, atau orang lain yang memiliki izin sah dari pemilik atau operator sistem untuk memberikan izin program komputer yang telah diakses, komputer, sistem komputer, atau jaringan komputer.

(b) Program komputer, komputer, sistem komputer, atau jaringan komputer diakses dan telah melewati prosedur pre-program sebelumnya dan akan menampilkan bulletin, perintah, atau pesa lain sebelum akses berhasil dilaksanakan yang mana orang yang bertanggung jawab akan percaya mengidentifikasi program komputer,

komputer, sistem komputer, atau jaringan komputer seperti dalam domain publik.

(c) Akses dicapai tanpa menggunakan satu set instruksi, kode, atau program komputer yang mengabaikan, menipu, atau mengelak dari prosedur akses terprogram untuk program komputer, komputer, sistem komputer atau jaringan komputer.

(7) Pengadilan dapat memerintahkan seseorang yang didakwa melanggar pasal ini untuk membayar kembali Negara bagian ini atau pemerintah daerah di Negara bagian ini untuk biaya yang dikeluarkan sehubungan dengan pelanggaran dengan cara yang sama dengan biaya yang dapat diminta untuk diganti berdasarkan pasal 1 bab IX kode prosedur pidana, 1927 PA 175, MCL 769.1f.

(8) Seperti yang sudah disebutkan dalam bagian ini, "dakwaan sebelumnya" berarti pelanggaran atau percobaan pelanggaran bagian 145d *Michigan Penal Code*, 1931 PA 328, MCL 750.145d, atau pasal ini atau hukum yang mirip secara substansial di Amerika Serikat, Negara bagian lain, atau subdivisi politik Negara bagian lain.

D. Pengaturan mengenai Tindak Pidana, Pertanggungjawaban Pidana dan Pemidanaan dalam *Criminal Law of the People's Republic of Tiongkok*

Criminal Law of the People's Republic of Tiongkok adalah Kitab Undang-undang Hukum Pidana milik Tiongkok. *Cybercrime* di KUHP Tiongkok diatur dalam pasal 285 sampai dengan pasal 287.

1. *Article 285. Whoever violates state regulations and intrudes into computer systems within information concerning state affairs, of defense facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.*

   (Terjemahan Pasal 285)

   Barang siapa melanggar peraturan negara dan mengganggu sistem komputer dalam informasi mengenai urusan negara, atau fasilitas pertahanan, dan ilmu pengetahuan dan teknologi canggih dihukum hukuman penjara tetap tidak lebih dari 3 tahun atau hukuman penjara yang telah ditentukan secara tetap.

2. *Article 286. Whoever violates states regulations and deletes, alters, adds and interferes in computer information systems, caused abnormal operations of the systems and grave consequences, is to be sentenced to not more than*

five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds the data or applications programs installed in or processed and transmitted by the computer systems, and causes grave consequences is to be punished according to the first paragraph.

Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

(Terjemahan pasal 286)

Barang siapa melanggar peraturan Negara dan menghapus, mengubah, menambah, dan mencampuri sistem informasi komputer, menyebabkan operasi sistem yang tidak normal dan konsekuensi yang besar, dihukum tidak lebih dari 5 tahun penjara tetap atau penahanan pidana; jika konsekuensinya sangat serius, hukumannya tidak lebih dari 5 tahun penjara atau hukuman penjara yang telah ditentukan secara tetap.

Barang siapa yang melanggar peraturan Negara dan menghapus, mengganti, atau menambah data atau aplikasi program yang dipasangkan atau diproses dan ditransmisikan oleh sistem komputer, dan menyebabkan konsekuensi yang serius, dihukum menurut paragraf sebelumnya.

Barang siapa dengan siapa membuat dan menyebarkan virus komputer dan program lain yang menyabotase operasi normal sistem komputer dan menyebabkan konsekuensi serius dihukum sesuai dengan paragraf pertama.

3. *Article 287. Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.*

(Terjemahan pasal 287)

Barang siapa menggunakan komputer untuk penipuan uang, pencurian, korupsi, penyalahgunaan dana publik, mencuri rahasia Negara, atau perbuatan pidana lain didakwa dan dihukum sesuai dengan peraturan yang relevan.

Dalam pasal 287, terdapat ketentuan tentang perbuatan pidana lain yang didakwa dan dihukum sesuai dengan peraturan yang relevan. Peraturan yang dimaksud adalah

pasal yang mengatur tentang perbuatan yang sama dengan pasal 287.

Undang-undang yang mengatur tentang cybercrime di Tiongkok hanya terdapat dalam KUHPnya dan hanya ada tiga pasal. Perbuatan yang dilarang pun juga terbatas, akses illegal yang termasuk di dalamnya pengrusakan sistem komputer, penyebaran virus yang merusak sistem komputer dan tindak pidana yang menyebabkan kerugian finansial yang dilakukan di internet. Tidak terdapat adanya peraturan yang melarang pornografi anak dalam KUHP Tiongkok, dan juga peraturan lain seperti adanya pencemaran nama baik, isu SARA dan lain-lain. Pasal 287 pun juga tidak memberikan hukuman secara spesifik, bahkan merujuk kepada peraturan lain yang mengatur sanksi pada tindak pidana tersebut.

E. Pengaturan tentang Tindak Pidana, Pertanggungjawaban Pidana, dan Pemidanaan dalam Tindak Pidana *Cyber* dalam Regulasi Positif Indonesia saat ini (Ius Constitutum)

Hukum yang mengatur tentang *cybercrime* terdapat dalam UU ITE. Khususnya pasal 27 sampai dengan pasal 37. Ketentuan pidananya diatur dalam pasal 45 sampai dengan pasal 52.

Perbuatan yang dilarang dalam UU ITE terdapat dalam pasal berikut:

1. Pasal 27:

a. Ayat (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;
b. Ayat (2): 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 perjudian;
c. Ayat (3): 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 penghinaan dan/atau pencemaran nama baik;
d. Ayat (4): 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 pemerasan dan/atau pengancaman;

2. Pasal 28:
   a. Ayat (1): Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang

mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

b. Ayat (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 antar golongan (SARA).

3. Pasal 29:

   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.

4. Pasal 30:

   a. Ayat (1): Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

   b. Ayat (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.

   c. Ayat (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.

5. Pasal 31:
    a. Ayat (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.
    b. Ayat (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 keadaan 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.
    c. Ayat (3): Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

d. Ayat (4): Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Undang-undang.

6. Pasal 32:
   a. Ayat (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 public.
   b. Ayat (2): Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer onformasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.
   c. Ayat (3): Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang emngakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh public dengan keutuhan data yang tidak sebagaimana mestinya.
7. Pasal 33:

   Setiap orang 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.

8. Pasal 34:
    a. Ayat (1): Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
        (1) Perangkat keras atau perangkat lunak komputer yang dirancang ataus secara khusus dikembangkan untuk menfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33;
        (2) 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.
    b. Ayat (2): Tindakan sebgaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian sistem elektronik, untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.
9. Pasal 35:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipilasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen lektronik tersebut dianggap seolah-olah data yang otentik.

10. Pasal 36:

    Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain.

Pasal 27 ayat (4) dan pasal 29 UU ITE merupakan pasal turunan dari KUHP pasal 310 dan 311 yang berbunyi sebagai berikut:

1. Pasal 310 KUHP:
    a. Ayat (1): Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah;
    b. Ayat (2): Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis

dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah;

c. Ayat (3): Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri;

2. Pasal 311 KUHP:

a. Ayat (1): Bila yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan kebenaran tuduhannya itu namun ia tidak dapat membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahuinya, maka dia diancam karena melakukan fitnah dengan pidana penjara paling lama empat tahun;

b. Ayat (2): Pencabutan hak-hak tersebut dalam pasal 35 ayat (1) sampai dengan (3) dapat dijatuhkan.

Sedangkan pasal 32 ayat (2) juga merupakan turunan dari pasal 362 KUHP tentang pencurian, yang berbunyi sebagai berikut:

> "Barangsiapa mengambil suatu barang, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk memilikinya secara melawan hukum, diancam karena pencurian dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah."

Selanjutnya, dalam UU ITE diatur ketentuan pidana terhadap perbuatan yang dilarang. Ketentuan pidana ini terdapat dalam pasal 45

sampai dengan 52. Namun dengan adanya UU Perubahan UU ITE, pasal 45 dan pasal 46 disisipkan menjadi satu pasal, yaitu pasal 45A dan pasal 45B. Ketentuan pidana tersebut adalah sebagai berikut:

1. Pasal 45A:
    a. Ayat (1): Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
    b. Ayat (2): Setiap Orang yang 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) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
2. Pasal 45B

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

pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

3. Pasal 46
   a. Ayat (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 Rp600.000.000,00 (enam ratus juta rupiah).
   b. Ayat (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).
   c. Ayat (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).
4. 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 Rp800.000.000,00 (delapan ratus juta rupiah).

5. Pasal 48

   a. Ayat (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 Rp2.000.000.000,00 (dua miliar rupiah).

   b. Ayat (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 Rp3.000.000.000,00 (tiga miliar rupiah).

   c. Ayat (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 Rp5.000.000.000,00 (lima miliar rupiah).

6. Pasal 49

   Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

7. Pasal 50

   Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

8. Pasal 51
    a. Ayat (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 Rp12.000.000.000,00 (dua belas miliar rupiah).
    b. Ayat (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 Rp12.000.000.000,00 (dua belas miliar rupiah).
9. Pasal 52
    a. Ayat (1): Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau pornografi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
    b. 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.
    c. 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.

d. 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.

F. Perbandingan CoC, MCL, Criminal Law on People's Republic of Tiongkok dan UU ITE

Keempat undang-undang ini walaupun mengatur hal yang sama memiliki perbedaan yang cukup besar satu sama lain. Dengan CoC sebagai acuan, pasal-pasal yang terdapat dalam CoC diintegrasikan menjadi peraturan nasional yang dipengaruhi oleh kebudayaan masing-masing negara. Indonesia misalnya, mengintegrasikan CoC dengan memasukkan norma-norma kesusilaan dan agama, yang tentunya berbeda dengan Michigan dan Tiongkok, yang nilai kesusilaan dan agamanya tidak dijunjung sekuat di Indonesia. Secara keseluruhan, MCL memiliki isi yang hampir sama dengan CoC. Namun berbeda dengan Criminal Law on People's Republic of Tiongkok, yang hanya terdapat 3 pasal yang mengatur tentang *cybercrime.*

1. Perbandingan asas hukum CoC, Michigan, Indonesia dan Tiongkok

   a. Asas kebebasan berpendapat

      Michigan yang merupakan negara bagian Amerika Serikat menganut paham liberal. Dalam pasal 1 bagian 5 Konstitusi Michigan tahun 1963, terdapat asas kebebasan berekspresi yang dilindungi oleh negara. Kebebasan berekspresi ini tidak bisa dikenai hukuman apa pun. Berbeda dengan Indonesia, asas kebebasan berekpresinya dibatasi dengan adanya larangan muatan SARA dan pencemaran nama baik. Apabila terbukti terdapat muatan SARA dan pencemaran nama baik, maka pelaku dapat dikenai sanksi sesuai dengan pasal 45A UU ITE. Di Tiongkok, yang terjadi belakangan ini adalah kebebasan berekspresinya dibatasi oleh pemerintah dengan undang-undang yang baru.

   b. Asas *equality before the law*

      Asas ini diberlakukan di seluruh undang-undang yang diteliti dalam skripsi ini. dalam MCL pun tidak ada perbedaan bagi pelaku percobaan *cybercrime*, bahkan hukumannya disamakan dengan tindak pidana yang telah terlaksana sempurna.

2. Perbandingan Tindak Pidana MCL, UU ITE dan *Criminal Law on People's Republic of Tiongkok.*

   Di MCL, tindak pidana cyber yang diuraikan merupakan tindak pidana yang kurang lebih sama dengan CoC. Sedangkan di *Criminal Law on People's Republic of Tiongkok,* tindak pidananya hanya sebatas tindak pidana umum yang dilakukan di internet, tidak menguraikan tindak pidana khusus seperti yang sudah terdapat dalam CoC. Lain pula dengan Indonesia. Indonesia pada dasarnya juga mengintegrasikan CoC ke dalam UU ITE, namun dengan penambahan norma kesusilaan dan norma keagamaan. Salah satu perbedaan yang kuat terdapat dalam pasal 27 ayat (1), yaitu tentang kesusilaan. Kesusilaan yang dimaksud di sini adalah tindakan asusila yang dilakukan oleh orang dewasa dan cakap hukum maupun anak. Di Michigan dan Tiongkok tidak mengatur adanya tindakan asusila yang dilakukan oleh orang dewasa. Orang dewasa dianggap cakap hukum untuk memberikan persetujuan dalam melakukan perbuatan yang dirasa melanggar kesusilaan, namun apabila perbuatan asusila dilakukan kepada anak, seperti pelecehan seksual, eksplotasi seksual dan sebagainya, anak dianggap belum bisa memberikan persetujuan terhadap hal tersebut.

Tindak pidana lain yang sangat berbeda adalah kegiatan yang berkaitan dengan kebebasan berekspresi. Sejauh ini, Indonesia selalu menekankan untuk tidak membuat pesan yang bermuatan SARA dan tidak melakukan pencemaran nama baik. Terdapat kebebasan berekspresi untuk menyampaikan pendapat kepada suatu topik atau kepada seseorang, tanpa menyinggung SARA maupun nama baik seseorang. Mengenai nama baik seseorang, hal ini agak sulit dibuktikan karena cara penyampaian setiap orang sangat berbeda dan cara orang memahami penyampaian tersebut juga berbeda. Di Michigan, terdapat kebebasan berekspresi yang sebebas-bebasnya. Negara melindungi hak kebebasan berekspresi ini. Hukum tidak dapat diimplementasikan kepada orang yang memberikan pendapatnya, apabila terjadi pencemaran nama baik, atau pun terdapat muatan SARA. Di Tiongkok, belakangan ini terdapat undang-undang baru yang dirasa semakin membatasi kebebasan rakyat berekspresi.

Berdasarkan seluruh penjelasan di atas, dapat dibuat tabel perbandingan sebagai berikut.

UNIVERSITAS KATOLIK
SOEGIJAPRANATA

TABEL 1.1. Tabel Perbandingan MCL, UU ITE dan Criminal Law on People of Republic of Tiongkok

UNSUR	NEGARA		
	Michigan (USA)	**Indonesia**	**TIongkok**
PELAKU **(Subjek)**	Seseorang yang berusia cukup dan cakap hukum	Seseorang yang berusia cukup dan cakap hukum	Seseorang yang berusia cukup dan cakap hukum
Perbuatan Melawan Hukum (menurut CoC)			
1. Illegal access (Art. 2)	Bagian 752.794 Bag. 4. Seseorang dilarang mengakses atau membuka suatu akses secara sengaja untuk masuk ke dalam suatu program komputer, komputer, sistem komputer, atau jaringan komputer untuk merancang atau menjalankan sebuah skeman atau berbuat licik dengan tujuan untuk menipu untuk mendapatkan uang, benda-benda kepemilikan, atau pelayanan dengan kepura-puraan yang curang, perwakilan, atau kesepakatan.	Pasal 30 UU ITE (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	Pasal 285 Barang siapa melanggar peraturan negara dan mengganggu sistem komputer dalam informasi mengenai urusan negara, atau fasilitas pertahanan, dan ilmu pengetahuan dan teknologi canggih dihukum hukuman penjara tetap tidak lebih dari 3 tahun atau hukuman penjara yang telah ditentukan secara tetap.

		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.	
(4) Illegal interception (Art. 3)	Bagian 752. 795 perbuatan terlarang Bag. 5. Seseorang dilarang tanpa sengaja dan tanpa hak atau melebihi hak sahnya melakukan yang ada di bawah ini: G. Mengakses atau membuat akses ke program komputer, komputer, sistem komputer, atau jaringan komputer untuk memperoleh, mengubah, merusak, menghapus, atau menghancurkan harta benda atau kegunaan lain atau jika tidak menggunakan pelayanan suatu program komputer, komputer, sistem komputer, atau jaringan komputer. H. Memasukkan atau menempelkan	Pasal 31 UU ITE e. 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. f. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi	Pasal 286 (paragraph 1) Barang siapa melanggar peraturan Negara dan menghapus, mengubah, menambah, dan mencampuri sistem informasi komputer, menyebabkan operasi sistem yang tidak normal dan konsekuensi yang besar, dihukum tidak lebih dari 5 tahun penjara tetap atau penahanan pidana; jika konsekuensinya sangat serius, hukumannya tidak lebih dari 5 tahun penjara atau hukuman penjara yang telah

	atau dengan sadar membuat kesempatan masuknya atau menempelnya instruksi yang tidak diketahui dan tidak diinginkan pada program komputer, komputer, sistem komputer, atau jaringan komputer, yang dimaksudkan untuk memperoleh, mengubah, merusak, menghapus, mengganggu atau menghancurkan harta benda atau menggunakan fungsi program komputer, komputer, sistem komputer, atau jaringan komputer. Subbagian ini tidak melarang tindakan yang dilindungi di bawah bagian 5 Pasal I konstitusi Negara bagian tahun 1963 atau di bawah amandemen pertama konstitusi Amerika Serikat.	informasi elektronik dan/atau dokumen elektronik yang tidak bersifat public dari, ked an 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. g. Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang	ditentukan secara tetap.

		kewenangannya ditetapkan berdasarkan undang-undang. h. Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Undang-undang.	
(5) Data Interference (Art. 4)		Pasal 32 UU ITE d. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, meindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik public. e. Setiap orang dengan	Pasal 286 (paragraf 2) Barang siapa yang melanggar peraturan Negara dan menghapus, mengganti, atau menambah data atau aplikasi program yang dipasangkan atau diproses dan ditransmisikan oleh sistem komputer, dan menyebabkan konsekuensi yang serius, dihukum menurut paragraf sebelumnya.

		sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer onformasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak. f. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang emngakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh public dengan keutuhan data yang tidak sebagaimana mestinya.	
(6) System interference (Art. 5)		Pasal 32: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya	Pasal 286 (paragraph 1) Barang siapa melanggar peraturan Negara dan menghapus, mengubah, menambah, dan mencampuri

		sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.	sistem informasi komputer, menyebabkan operasi sistem yang tidak normal dan konsekuensi yang besar, dihukum tidak lebih dari 5 tahun penjara tetap atau penahanan pidana; jika konsekuensinya sangat serius, hukumannya tidak lebih dari 5 tahun penjara atau hukuman penjara yang telah ditentukan secara tetap. - Pasal 286 (paragraph 2) Barang siapa dengan siapa membuat dan menyebarkan virus komputer dan program lain yang menyabotase operasi normal sistem komputer dan menyebabkan konsekuensi serius dihukum sesuai dengan paragraf pertama.
(7) Misuse of devices (Art. 6)	Tidak atau belum diatur dalam Michigan Compiled Law.	Pasal 34: (3) Setiap orang 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 ataus secara khusus dikembangkan untuk menfasilitasi 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. (4) Tindakan sebgaimana dimaksud pada ayat (1)	

		bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian sistem elektronik, untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.	
(8) Computer-related forgery (Art. 7)	Bagian 752.796 penggunaan program komputer, sistem komputer, atau jaringan komputer untuk melakukan tindakan kriminal. Bag. 6. (4) Seseorang dilarang menggunakan program komputer, sistem komputer, atau jaringan komputer untuk melakukan, mencoba melakukan, bekerja sama melakukan, atau mengajak orang lain untuk melakukan tindak kriminal. (5) Bagian ini tidak menghentikan orang dari dibebani, didakwa, atau dihukum karena pelanggaran hukum yang dilakukan oleh orang lain saat melanggar atau mencoba melanggar bagian ini, termasuk	Pasal 35: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipilasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen lektronik tersebut dianggap seolah-olah data yang otentik.	Pasal 287 Barang siapa menggunakan komputer untuk penipuan uang, pencurian, korupsi, penyalahgunaan dana publik, mencuri rahasia Negara, atau perbuatan pidana lain didakwa dan dihukum sesuai dengan peraturan yang relevan.

	dengan pelanggaran yang mendasar. (6) Bagian ini diterapkan tanpa peduli apakah orang tersebut didakwa melakukan, mencoba melakukan, bekerja sama melakukan, atau mengajak orang lain melakukan degan pelanggaran yang mendasar.		
(9) Computer-related fraud (Art. 8)		Pasal 28 c. Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. d. 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 antar golongan	Pasal 287 Barang siapa menggunakan komputer untuk penipuan uang, pencurian, korupsi, penyalahgunaan dana publik, mencuri rahasia Negara, atau perbuatan pidana lain didakwa dan dihukum sesuai dengan peraturan yang relevan.

		(SARA).	
(10) Offences related to child pornography (Art. 9)		Dalam UU ITE, tidak diatur secara langsung tindak pidana pornografi yang melibatkan anak. Namun dalam pasal 52 diatur hukumannya apabila terjadi perbuatan kesusilaan dan pornografi anak.	Tidak atau belum diatur dalam KUHP Tiongkok.
Sanksi Hukum **(Menurut hukum nasional masing-masing Negara)**			
1. Illegal access (Art. 2)	➔ 752.797 Hukuman, dakwaan prioritas, anggapan, perintah pengembalian, ketentuan lain. Bag. 7. (1) Seseorang yang melanggar pasal 4 dinyatakan bersalah melakukan tindak pidana sebagai berikut: (e) Jika pelanggaran melibatkan jumlah yang apabila dikumpulkan mencapai kurang dari $200.00, orang tersebut dinyatakan bersalah akan tindak pidana ringan yang harus dihukum dengan hukum	Pasal 46 Ayat (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 Rp600.000.000,00 (enam ratus juta rupiah). Ayat (2): Setiap Orang yang memenuhi unsur sebagaimana	

	penjara tidak lebih dari 93 hari atau denda tidak lebih dari $500.00 atau 3 kali dari jumlah yang diakumulasikan, yang mana lebih besar, atau hukum penjara dan denda. (f) Jika hal berikut berlaku, seseorang yang bersalah atas tindak pidana ringan yang harus dihukum dengan hukum penjara tidak lebih dari 93 hari atau denda tidak lebih dari $500.00 atau 3 kali dari jumlah yang diakumulasikan, yang mana lebih besar, atau hukum penjara dan denda: i. Pelanggaran melibatkan total jumlah $200.00 atau lebih namun kurang dari $1,000.00. ii. Seseorang melanggar pasal ini dan sudah didakwa terlebih dahulu. (g) Jika hal berikut berlaku, maka orang yang bersalah atas tindak pidana berat yang harus dihukum tidak lebih dari 5 tahun atau denda tidak lebih dari $10,000.00 atau 3 kali lebih besar dari jumlah total yang dikumpulkan, yang mana	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). Ayat (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).	

	lebih besar, atau hukum penjara dan denda: i) Pelanggaran melibatkan jumlah keseluruhan sebesar $1,000.00 atau lebih namun kurang dari $20,000.00. ii) Orang tersebut sudah didakwa dengan 2 dakwaan. iii)Jika hal berikut berlaku, maka orang yang bersalah atas tindak pidana berat harus dihukum tidak lebih dari 10 tahun atau denda 3 kali lebih besar dari jumlah total yang dikumpulkan, yang mana lebih besar, atau hukum penjara dan denda: 1. Pelanggaran tersebut melibatkan jumlah keseluruhan $20,000.00 atau lebih. 2. Orang tersebut sudah didakwa dengan 3 dakwaan.		
2. Illegal interception (Art. 3)		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 Rp800.000.000,00 (delapan ratus juta rupiah).	
3. Data Interference (Art. 4)	(1) Seseorang yang melanggar pasal 5 dinyatakan bersalah melakukan tindak pidana sebagai berikut: (c) Seperti pengecualian di subbagian (b), seseorang yang dinyatakan bersalah karena tindak pidana berat harus dihukum hukuman penjara tidak lebih dari 5 tahun atau denda tidak lebih dari $10,000.00, atau keduanya. (d) Jika orang tersebut sudah didakwa dengan dakwaan lain sebelumnya, orang tersebut dinyatakan bersalah atas tindak pidana berat harus dihukum hukuman penjara tidak lebih dari 10 tahun dan denda tidak lebih dari $50,000.00, atau keduanya.	Gangguan data ketentuannya diatur dalam 2 pasal, yaitu pasal 32 dan pasal 35. Pasal 32 hukumannya diatur dalam pasal 48, sedangkan pasal 35 diatur dalam pasal 51. Pasal 48: Ayat (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 Rp2.000.000.000,00 (dua miliar rupiah). Ayat (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 Rp3.000.000.000,00 (tiga miliar rupiah). Ayat (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 Rp5.000.000.000,00 (lima miliar rupiah). Pasal 51 Ayat (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 Rp12.000.000.000,00 (dua belas miliar rupiah).	

		Ayat (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 Rp12.000.000.000,00 (dua belas miliar rupiah).	
(2) System interference (Art. 5)	Pasal 752.796a, pelanggaran terhadap 752.795a (4) Seseorang yang melanggar bagian 5a dinyatakan bersalah karena berikut ini: (d) Pelanggaran pertama, dianggap kejahatan ringan yang harus dihukum dengan hukuman penjara tidak lebih dari 1 tahun atau denda tidak lebih dari $10,000.00, atau keduanya. (e) Pelanggaran kedua, dianggap kejahatan besar yang harus dihukum dengan hukuman penjara tidak lebih dari 2 tahun atau denda tidak lebih dari $20,000.00, atau keduanya. (f) Pelanggaran ketiga atau seterusnya, dianggap kejahatan	Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).	Pelaku yang mengganggu sistem komputer dalam *Criminal Law of People's Republic of Tiongkok* dihukum 3 tahun penjara atau hukuman yang ditentukan oleh hakim.

	besar yang harus dihukum dengan hukuman penjara tidak lebih dari 3 tahun atau denda $30,000.00, atau keduanya. (5) Seseorang tidak melanggar bagian 5a karena orang tersebut adalah penghubung antara pengirim dan penerima dalam pengiriman pesan elektronik yang melanggar bagian 5a atau secara tidak sadar membantu pengiriman pesan elektronik ke jaringan komputer orang lain atau fasilitas yang melanggar bagian 5a. (6) Ini adalah pembelaan terhadap tindakan yang dilakukan di bawah bagian ini bahwa komunikasi tersebut ditransmisikan secara tidak sengaja. Pembuktian bahwa komunikasi yang ditransmisikan secara tidak sengaja dibebankan kepada pengirim.		
(3) Misuse of devices (Art. 6)		Pasal 50 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling	

		lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).	
(4) Computer-related forgery (Art. 7)		Pasal 45A Ayat (1): Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Ayat (2): Setiap Orang yang 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) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).	
(5) Computer-related fraud (Art. 8)		Tidak atau belum diatur dalam UU ITE.	
(6) Offences related to child pornography (Art. 9)		Segala perbuatan dalam pasal 27 ayat (1) dan apabila terdapat pornografi anak, dikenakan pemberatan sepertiga dari pidana pokok.	

G. Sumbangan Formulasi Hukum Pidana *Cyber Di* As Dan Tiongkok Terhadap Pembentukan Hukum *Cyber* Indonesia (*Ius Constituendum*)

UU ITE secara keseluruhan telah mengadopsi CoC untuk mencegah tindakan-tindakan yang dirasa membahayakan negara. Akses illegal, penggunaan program komputer untuk merusak sistem komputer, pesan-pesan yang memuat pelanggaran kesusilaan, pencemaran nama baik, konten perjudian, dan lain sebagainya sebagaimana diatur dalam UU ITE merupakan bentuk dari integrasi CoC.

Dalam MCL, hak kebebasan berekspresi dilindungi oleh negara. Hak tersebut merupakan hak yang tidak dapat diganggu gugat, walaupun dalam kegiatan berekspresi tersebut menyinggung suatu ras atau suku tertentu, atau bahkan terindikasi mencemarkan nama baik seseorang. Hak kebebasan berekspresi di Indonesia dibatasi dengan dilarangnya membawa isu SARA dan dilarang mencemarkan nama baik, dan apabila terdapat bukti bahwa pelaku membawa isu SARA dan mencemarkan nama baik seseorang, dihukum sesuai dengan dengan Pasal 45 jo. Pasal 27 ayat (3) UU ITE. Dalam Pasal 27 ayat (3) UU ITE, belum dijelaskan secara terperinci mengenai batasan-batasan antara mengajukan kritik, koreksi, dan mencemarkan nama baik. Dengan adanya pasal ini, rakyat Indonesia seolah dibatasi dalam mengemukakan pendapat.

Sumbangan yang dapat diberikan kepada Indonesia adalah konsep kebebasan berekspresi yang dianut oleh Michigan. Hak kebebasan berekspresi selayaknya bebas mengemukakan pendapat apa saja, tanpa

batasan SARA maupun pencemaran nama baik. Pencemaran nama baik maupun isu SARA pada dasarnya agak sulit dibuktikan, karena tergantung dari cara penyampaian dan cara pemahaman seseorang. Sebagai contoh, yang baru saja terjadi, yaitu vlog (*video blog*) milik Kaesang Pangarep yang sebenarnya hanya menyatakan fakta Pilkada 2017 lalu yang baru saja terjadi, namun ada pula orang yang merasa perkataan Kaesang menyinggung isu SARA.

Hal lain yang patut diadopsi ialah penguatan pengaturan mengenai pornografi anak sebagaimana ditentukan dalam CoC dan pengaturan dari US dan Tiongkok. Pengaturan mengenai pornografi anak secara *online* akan ikut memperkuat regulasi lainnya seperti regulasi mengenai tindak pidana pornografi dan regulasi mengenai tindak pidana perdagangan orang, selain itu juga memperkuat pemberatan hukuman bagi pelaku pornografi anak. Menurut Penulis, hukuman bagi pelaku pornografi anak masih kurang dibandingkan dengan pornografi orang dewasa, sehingga diperlukan penegasan dalam tindak pidana tersebut.