UPAYA PENANGGULANGAN TINDAK PIDANA MAYANTARA (*CYBER CRIME*)[1]

Daniel F. T. Popal [2]
franciscotumuyu@gmail.com
Debby Telly Antouw [3]
Jolly Ken Pongoh [4]

ABSTRAK

Tujuan penelitian adalah untuk mengkaji bentuk-bentuk tindak pidana *Cybercrime* di Indonesia dan untuk mengkaji upaya pencegahan dan penanggulangan *cybercrime*. Dengan metode penelitian yuridis normatif disimpulkan : 1. Perkembangan teknologi yang semakin cepat dan kemajuan ilmu pengetahuan tidak dapat disangkal mengakibatkan munculnya kejahatan-kejahatan atau tindak pidana yang berkaitan dengan kecanggihan teknologi atau yang dikenal dengan kejahatan/tindak pidana *cyber crime*, dimana bentuk-bentuknya begitu banyak dan beragam seperti *identity theft*, kejahatan *phishing*, kejahatan *carding*, serangan *ransomware*, penipuan *online*, SIM *swap*, peretasan situs dan *email*, kejahatan *skimming*, OTP *Fraud*, pemalsuan data atau data *forgery*, kejahatan konten ilegal, teroris dunia maya atau *cyber terorism*, mata-mata atau *cyber espionage*, dan menjiplak situs orang lain. Dari beragam bentuk *cyber crime* ini yang sering terjadi adalah bentuk akses ilegal (*carding*), *phishing*, penipuan OTP, kejahatan konten ilegal, membajak sistem komputer dan *cyber terorism*. 2. Upaya penanggulangan *cybercrime* dengan sarana penal, yaitu selain sudah diatur dalam pasal-pasal yang ada dalam KUHP seperti Pasal 362 tentang Pencurian, Pasal 378 tentang Penipuan dan Pasal 263 tentang Pemalsuan identitas dengan ancman hukuman yang ada, juga dengan dibelakukannya UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang ITE khususnya dalam Pasal 27 sampai dengan Pasal 37 tentang Perbuatan yang dilarang dan dalam Pasal 45 sampai dengan Pasal 52 tentang ancaman penjara dengan mengenakan ancaman hukuman penjara paling berat 12 (dua belas) tahun dan hukuman denda paling banyak Rp. 2.000.000.000,00 (dua milyar rupiah).

Kata Kunci : tindak pidana mayantara

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi informasi (*information technology*) memegang peran yang penting, baik di masa kini maupun di masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya. Kedua, adalah memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.[5]

Kesenjangan antara negara kaya (maju) dan negara miskin (miskin sekali atau negara berkembang) dalam bidang teknologi informasi sangat lebar jaraknya.[6] Perkembangan teknologi umumnya dan internet pada khususnya tidak bisa dinikmati oleh orang-orang biasa seperti sekarang ini, tetapi bermain dalam tingkat elit. Pengabdian total dunia teknologi terhadap kekuasaan negara adalah inovasi perangkat perang sehingga muncul dari setiap akumulasi kekuasaan kaum bermodal melalui negara adalah perang.

Sesudah perang dingin, internet tidak lagi digunakan untuk kepentingan militer, tetapi beralih fungsi menjadi sebuah media yang mampu membawa perubahan dalam kehidupan manusia. Internet tidak lagi hanya digunakan oleh kalangan militer, pemerintah dan ilmuwan, tetapi juga digunakan oleh pelaku bisnis, politikus, sastrawan, budayawan, musikus bahkan para penjahat dan teroris. Internet mulai digunakan sebagai alat propaganda politik, transaksi bisnis atau perdagangan, sarana pendidikan, kesehatan, manufaktur, perancangan, pemerintahan, pornografi dan kejahatan lain.

Kehadiran internet telah membuka cakrawala baru dalam kehidupan manusia. Internet merupakan sebuah ruang informasi dan komunikasi yang menjanjikan, menembus batas-batas antar negara dan mempercepat penyebaran dan pertukaran ilmu dan gagasan di kalangan ilmuwan dan cendekiawan di seluruh dunia. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan *'Cyberspace'*.

Cyberspace merupakan tempat kita berada ketika kita mengarungi dunia informasi global

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 16071101420
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Dari Pertemuan G-8 Okimawa, *Teknologi Informasi Yang Melaju Dan Tergilas*, Kompas, 23 Juli 2020, hlm.3.
[6] *Ibid.*

interaktif yang bernama internet.[7] Istilah ini pertama kali digunakan oleh William Gibson dalam novel fiksi ilmiahnya yang berjudul *Neuromancer*.[8] *Cyberspace* menampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat, melainkan realitas virtual (*virtual reality*), dunia maya, dunia yang tanpa batas. Inilah sebenarnya yang dimaksud dengan *borderless world*, karena memang dalam *cyberspace* tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat.[9] Sehingga penghuni-penghuninya bisa berhubungan dengan siapa saja dan di mana saja. Sebagaimana dikatakan oleh Bruce Sterling, *cyberspace* menawarkan manusia untuk 'hidup' dalam dunia alternatif, sebuah dunia pelayanan dapat mengambil alih dan menggantikan realitas yang ada, yang lebih menyenangkan dari kesenangan yang ada, yang lebih fantatis dari fantasi yang ada, yang lebih masyarakat dalam berbagai sisi realitas baru yang tidak pernah dibayangkan sebelumnya, yang penuh dengan harapan, kesenangan, kemudahan dan pengembaraan, seperti *teleshopping, teleconference, teledildonic, virtualcafe, virtual architecture, virtual museum, cybersex, cyberparty dan cyberorgasm.*[10]

Proses *cybernation* yang menimbulkan harapan akan kemudahan, kesenangan dan kesempatan itu ternyata tidak selamanya demikian karena dalam *cyberspace* juga terdapat sisi gelap yang perlu kita perhatikan. Kecemasan terhadap *cybercrime* telah menjadi perhatian dunia, terbukti dengan dijadikannya masalah *cybercrime* sebagai salah satu topik bahasan pada Kongres Perserikatan Bangsa-Bangsa (PBB) mengenai *The Prevention of Crime And The Treatment of Offender* Ke-8 tahun 1990 di Havana, Kuba dan kongres ke-10 di Wina. Pada kongres ke-8 Perserikatan Bangsa-Bangsa (PBB) memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer (*computer related crime*), sedangkan pada kongres ke-10 di Wina, *cybercrime* dijadikan sebagai topik bahasan tersendiri dengan judul *Crimes Related To Computer Network.*

Tidak semua negara di dunia memberikan perhatian yang lebih besar tentang masalah *cybercrime* dan memiliki peraturannya (kecuali negara-negara maju dan beberapa negara berkembang). Hal ini disebabkan oleh tingkat kemajuan dan perhatian dari hukum dan teknologi.

Indonesia sebagai negara berkembang memang terlambat dalam mengikuti perkembangan teknologi informasi. Hal ini tidak lepas dari strategi pengembangan teknologi yang tidak tepat karena mengabaikan riset sains diikuti dengan penguasaan teknologi itu sendiri yang mengantarkan Inodnesia kepada negara yang tidak mempunyai basis teknologi.

Dari sekian banyak sisi gelap yang ada dalam *cyberspace*, yang paling banyak mendapat perhatian adalah perbuatan yang dilakukan oleh *cracker*. Fenomena ini dalam tahun-tahun terakhir ini memang mencemaskan karena mereka telah menggunakan keahliannya untuk melakukan kejahatan. Aktivitas *cracker* yang makin lama makin mencemaskan ini tentunya menimbulkan keragu-raguan pada manfaat internet yang telah ditawarkan. Berjuta-juta keuntungan yang diharapkan tentunya akan lenyap jika *cracker* dapat masuk dan merusak investasi yang telah ditanamkan pada pengembangan internet sebagai sarana aktivitas manusia. Untuk itu aktivitas *cracker* ini perlu dikriminalisasikan.

Kasus *cybercrime* di Indonesia semakin berkembang sejalan dengan perkembangan internet dan teknologi yang ada. Selain karena sistem keamanan yang lemah, kasus *cybercrime* di Indonesia terjadi karena kelalaian yang dilakukan oleh penggunanya sendiri. Contohnya yang pernah terjadi pada salah satu bank ternama di Indonesia, dimana pelaku mengirimkan email dan mengarahkan korban untuk mengisi data pribadi melalui situs palsu. Akibatnya korban mengalami kerugian dengan nominal yang sangat besar. Cara ini dinamakan teknik '*phising*', dimana '*phising* merupakan suatu metode yang dapat digunakan untuk mencuri data korban seperti *user id, password* dan lain-lain'. *Hacker* akan menyamar menggunakan form *login* atau situs palsu untuk memancing korban memasukkan data-data sensitif seperti *password* ataupun *user id*. Biasanya *hacker* menyebarkan *link* palsu melalui *email* atau melalui pesan *pop up* yang menyatakan bahwa anda memenangkan sebuah hadiah. Selanjutnya, *hacker* akan mengharuskan anda memasukkan data-data pribadi ke dalam situs palsu tersebut.[11] Contoh yang lain juga yaitu 'pembajakan situs *website* oleh serangan *web deface*'. *Web deface* merupakan salah satu kasus

[7] Armedi Mahzar, dalam kata pengantar Buku Jeff Zaleski, *Spiritualis Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia*, Mizan, Bandung, 1999, hlm.9.
[8] *Ibid*, hlm.53.
[9] Onno W. Purbo, *Perkembangan Teknologi Informasi dan Internet Di Indonesia*, Kompas, 28 Juni 2020, hlm.5.
[10] *Ibid.*
[11] Feradhita nkd, *Mengetahui 3 contoh Kasus Cyber crime di Indonesia*, diakses dari https://www.logique.co.ic pada tanggal 20 Desember 2022.

yang banyak terjadi di Indonesia. *Web deface* adalah kegiatan merubah tampilan suatu *website*, mulai dari halaman utama, *index file*, atau halaman lain yang masih terikat dengan *url website* tersebut. Peretas ini dapat melakukan aksi ini karena adanya celah keamanan pada sistem keamanan korban. *Website* yang pernah diretas adalah *website* yang dikelola oleh pemerintah.[12] Kasus yang lain juga yaitu, 'pencurian kartu kredit (*carding*)'. *Carding* merupakan kejahatan yang dilakukan dengan mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.[13]

Kitab Undang-Undang Hukum Pidana (KUHP) jelas telah mengatur tentang hal-hal sebagaimana disebutkan dalam kasus-kasus yang disebutkan seperti 'kasus pencurian kartu kredit, dimana dapat diterapkan pasal-pasal tentang 'Penipuan' dalam Pasal 378 KUHP, tentang 'pencurian' dalam Pasal 362 KUHP dan tentang 'Pemalsuan identitas' dalam Pasal 263 KUHP dan UU ITE No. 11 Tahun 2008 yang dirubah dengan UU No 19 Tahun 2019 telah mengatur dengan jelas tentang hal-hal tersebut di atas sebagaimana disebutkan dalam Pasal 27 sampai dengan Pasal 37 tentang perbuatan yang dilarang yang berkaitan dengan informasi dan elektronik yaitu berupa perbuatan 'mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik'.

B. Rumusan Masalah

1. Bagaimana bentuk-bentuk tindak pidana *cybercrime* di Indonesia?
2. Bagaimanakah upaya pencegahan dan penanggulangan *cybercrime* di Indonesia?

C. Metode Penelitian

Penelitian ini adalah penelitian hukum normatif atau penelitian hukum kepustakaan.

PEMBAHASAN

A. Bentuk-bentuk Tindak Pidana *Cybercrime* di Indonesia

Aktivitas di internet tidak bisa dilepaskan dari manusia dan akibat hukumnya terhadap manusia yang ada di dalam kehidupan nyata (*real life/ physical world*), sehingga muncul pemikiran mengenai perlunya aturan hukum yang mengatur aktivitas tersebut. Internet memiliki karakteristik yang berbeda dengan dunia nyata sehingga muncul pro dan kontra mengenai bisa tidaknya hukum tradisional/konvensional (*the existing law*) mengatur aktivitas tersebut atau perlu tidaknya aktivitas di internet diatur oleh hukum. Permasalahan sebenarnya bukan sebatas pada eksistensi hukum tradisional dalam mengatur aktivitas di internet, melainkan mempertanyakan eksistensi hukum tradisional dalam mengatur aktivitas di internet.[14]

Pro dan kotra tersebut disebabkan oleh dua (2) hal. Pertama, karakteristik aktivitas di internet yang bersifat lintas batas, sehingga tidak lagi tunduk pada batasan-batasan terirorial. Kedua, sistem hukum tradisisonal yang justru bertumpu pada batasan-batasan terirorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktivitas di internet.

Perbedaan pendapat yang menimbulkan kelompok yang pro dan kontra ini, terbagi menjadi tiga (3) kelompok, yaitu:

1. Kelompok pertama secara total menolak setiap usaha untuk membuat aturan hukum bagi aktivitas-aktivitas di internet yang didasarkan atas sistem hukum tradisional. Dengan pendirian seperti ini, maka menurut kelompok ini internet harus diatur sepenuhnya oleh sistem hukum baru yang didasarkan atas norma-norma hukum yang baru pula yang dianggap sesuai dengan karakteristik yangmelekat pada internet. Kelemahan utama dari kelompok ini adalah mereka menafsirkan fakta, meskipun aktivitas di internet itu sepenuhnya beroperasi secara virtual, tetapi masih tetap melibatkan masyarakat (manusia) yang hidup di dunia nyata.
2. Kelompok kedua berpendapat bahwa penerapan sistem hukum tradisional untuk mengatur aktivitas-aktivitas di internet sangat mendesak untuk dilakukan. Perkembangan internet dan kejahatan yang melingkupinya begitu cepat sehingga yang paling mungkin untuk pencegahan dan penanggulangannya adalah dengan mengaplikasikan sistem hukum tradisional yang saat ini berlaku. Kelemahan utama dari kelompok ini merupakan kebalikan dari kelompok pertama, yaitu mereka menafsirkan fakta bahwa aktivitas-aktivitas di internet menyajikan realitas dan persoalan baru yang merupakan fenomena khas masyarakat informasi yang tidak sepenuhnya dapat direspon oleh sistem hukum nasional.
3. Kelompok ketiga tampaknya merupakan sistesis dari kedua kelompok di atas. Mereka

[12] *Ibid.*
[13] *Contoh Kasus Cybercrime Di Indonesia Dan UU ITE terkait*, diakses dari https://edybillstephen.ilearning.me pada tanggal 20 Desember 2022.
[14] Atip Latifulhayat, *Op-Cit*, hlm-4.

berpendapat bahwa aturan hukum yang akan mengatur mengenai aktivitas di internet harus dibentuk secara evolutif dengan cara menerapkan prinsip-prinsip *common law* yang dilakukan secara hati-hati dan dengan menitikberatkan pada aspek-aspek tertentu dalam aktivitas *cyberspace* yang menyebabkan kekhasan dalam transaksi-transaksi di internet. Kelompok ini memiliki pendirian yang cukup moderat dan realistis karena memang ada beberapa prinsip hukum tradisional yang dapat merespon persoalan hukum yang timbul dari aktivitas di internet. Di samping juga bahwa beberapa transaksi di internet tidak dapat sepenuhnya direspon oleh sistem hukum tradisional.[15]

Sehubungan dengan uraian di atas, menarik untuk disimak langkah-langkah yang ditempuh oleh empat puluh satu (41) negara yang tergabung dalam "Dewan Eropa" (*Council of Europe*) dalam melakukan harmonisasi kebijakan hukum pidana untuk menanggulangi *cybercrime* sebagai berikut:

1. Pada bulan Nopember 1996, '*European Committee on Crime Problems*' (CDPC) membentuk panitia ahli di bidang *cyber crime* yang kemudian disebut "*Committee of Experts on Crime in Cyber-Space*" (PCCY) dan berhasil menyusun "*Draft Convention on Cyber Crime*".
2. Pada bulan April 2000, draft konvensi itu dipubilkasikan lewat internet untuk bahan diskusi publik. Draft awal yang dipubilkasikan itu adalah Draft No. 19. Sampai dengan bulan Desember 2000 sudah menajdi Draft Nomor 25, dan pada bulan Pebruari 2001 telah berhasil disusun "*Draft Explanatory Memorandum*" terhadap draft konvensi tersebut. Pada bulan Mei 2001 berhasil disusun Draft Final dari konvensi itu beserta Memorandum Penjelasannya (yaitu Draft Nomor. 27) yang diajukan untuk mendapat persetujuan *European Committee on Crime Problem* (CDPC) pada pertemuan ke-50 (tanggal 18 – 22 Juni 2001).
3. Draft Konvensi *Cyber Crime* (CC) ini terdiri dari empat (4) bab:
   a. mengenai peristilahan,
   b. mengenai tindakan-tindakan yang diambil di tingakt nasional domestik (negara anggota) di bidang hukum pidana materil dan hukum acara,
   c. mengenai kerja sama internasional,
   d. ketentuan penutup.
4. Khusus dalam Bab II Bagian 1 diatur mengenai "Hukum Pidana Substantif/Materiel" yakni dalam Pasal 2 sampai dengan Pasal 13, dan diantaranya memuat ketentuan-ketentuan mengenai tindak pidana (Pasal 2 sampai dengan Pasal 11).[16]

Dari uraian di atas terlihat bahwa, untuk mengantisipasi penanggulangan *cyber crime* dengan hukum pidana, Dewan Eropa berusaha terlebih dahulu melakukan harmonisasi kebijakan penal melalui suatu konvensi. Draft konvensi itu sendiri dipersiapkan terlebih dahulu oleh tim ahli/pakar di bidang "*Cybercrime*", dan kemudian di sosialisasikan untuk menjadi bahan 'diskusi publik'. Setelah *Draft* Konvensi diperbaiki berulangkali dan disetujui negara anggota (sampai saat ini masih dalam proses), baru ditindaklanjuti/dituangkan dalam kebijakan legislasi masing-masing negara anggota.

Mengamati pengalaman Dewan Eropa dalam menyusun kebijakan kriminalisasi di bidang *cybercrime (CC)* seperti dikemukakan di atas, maka dalam rangka penyusunan tindak pidana (kebijakan kriminalisasi) seyogyanya ditempuh terlebih dahulu kajian mengenai:

1) harmonisasi materi/substansi tindak pidana, dan
2) harmonisasi kebijakan formulasi tindak pidana.

Kajian harmonisasi kedua masalah ini seyogyanya dilakukan baik di tingkat regional maupun internasional.

Untuk masalah pertama, perlu masukan dari para pakar di bidang teknologi informasi, karena tentunya mereka yang lebih mengetahui perbuatan-perbuatan apa dan bagaimana yang dipandang sangat merugikan/membahayakan sehingga patut dijadikan tindak pidana (di kriminalisasi). Di samping itu, perlu masukan dari berbagai kalangan mengenai 'kepentingan hukum' atau 'nilai-nilai apa' yang seyogyanya dilindungi dari pengaruh negatif/penyalahgunaan teknologi informasi di ruang maya (mayantara atau *cyberspace*). Untuk masalah kedua, perlu dikaji apakah kebijakan formulasi/legislasi tindak pidana di bidang teknologi informasi atau *cyber crime* ini, dimasukkan dalam undang-undang khusus atau di integrasikan ke dalam undang-undang yang berlaku umum yaitu Kitab Undang-Undang Hukum Pidana (KUHP). Sejak tahun 2008, masalah kedua tentang harmonisasi kebijakan formulasi tindak pidana di dunia maya sudah diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No. 19 Tahun 2016.

[15] *Ibid*, hlm.4-6.

[16] *Ibid*, hlm.241-243.

"Draft Convention on Cyber Crime" dari Dewan Eropa, menyebutkan ruang lingkup tindak pidananya mencakup:

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Termasuk kelompok delik ini adalah:
   a. mengakses sistem komputer tanpa hak;
   b. tanpa hak menangkap/mendengar pengiriman dan pemancaran data komputer yang tidak bersifat publik dengan alat bantu teknis;
   c. tanpa hak merusak / menghapus / mengubah data komputer;
   d. tanpa hak mengganggu / merintangi berfungsinya sistem komputer;
   e. menyalahgunakan perlengkapan komputer (termasuk program komputer, *password*, dan kode masuk).
2. Delik-delik yang berhubungan dengan komputer, yaitu melakukan pemalsuan dan penipuan dengan komputer;
3. Delik-delik yang bermuatan pornografi anak; dan
4. Delik-delik yang berhubungan dengan pelanggaran hak cipta.

Di Indonesia, dalam UU No. 19 Tahun 2016 menyebutkan bahwa *cyber crime* termasuk dalam perbuatan yang dilarang sebagai berikut:

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun;
2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sisztem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik;
3. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan.[17]

Perkembangan teknologi yang semakin cepat dan kemajuan ilmu pengetahuan mengakibatkan timbulnya beberapa jenis kejahatan *cyber crime*, dimana harus menjadi perhatian yang khusus dari masyarakat. Bentuk-bentuk kejahatan atau tindak pidana *cyber crime* tersebut, sebagai berikut:[18]

1. *Identity Theft*
2. Kejahatan *Phishing*
3. Kejahatan *Carding*
4. Serangan *Ransomware*
5. Penipuan *Online*
6. SIM Swap
7. Peretasan Situs dan *Email*
8. Kejahatan *Skimming*
9. OTP *Fraud*
10. Pemalsuan Data atau Data *Forgery*
11. Kejahatan Konten Ilegal
12. Teroris Dunia Maya atau *Cyber Terorism*
13. Mata-mata atau *Cyber Espionage*
14. Menjiplak Situs Orang Lain

Dari 14 jenis kejahatan cyber crime sebagaiman sudah disebutkan di atas, saat ini yang sering terjadi adalah bentuk-bentuk *cyber crime* berupa: *phising*, bertransaksi ilegal (*carding*), membajak sistem komputer dan peretasan *website* atau situs oarang lain.

B. Upaya Penanggulangan Tindak Pidana *Cybercrime* di Indonesia.

Indonesia di dalam membuat Undang-Undang di bidang *cybercrime* ternyata menggunakan model *'umbrella provision'* sehingga ketentuan *cybercrime* tidak dalam perundang-undangan tersendiri, tetapi diatur secara umum dalam Undang-Undang Tentang Informasi Dan Transaksi Elektronik No. 11 Tahun 2008 yang telah diubah dengan UU No. 19 Tahun 2016.

Upaya penanggulangan tindak pidana/kejahatan *cybercrime* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik yang diubah dengan UU No. 19 Tahun 2016 tertuang dalam Bab VII dengan judul "Perbuatan Yang Dilarang", diatur mulai dari Pasal 27 sampai dengan Pasal 37. Bab VII Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik yang telah diubah dengan UU No. 19 Tahun 2016 ini pada intinya memuat perumusan tindak pidana seperti terdapat dalam konvensi *Cyber Crime* Dewan Eropa (*Council of Europe Cyber Crime Convention*, untuk selanjutnya disebut Konvensi *Cyber crime (CC*) yang telah ditanda tangani di Budapest pada tanggal 23 Nopember 2001, yaitu:
Pasal 27:

(1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.
(2) 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.
(3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan

[17] 14 Jenis *Cyber crime*, Kejahatan Internet Yang Merugikan, *Op-Cit.*
[18] *Ibid.*

dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

(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.

Terhadap Pasal 27 ayat (3) UU No. 11 Tahun 2008 ini, oleh UU No 19 Tahun 2016 tentang Perubahan atas No. 11 Tahun 2008, disebutkan bahwa:

1. 'Untuk menghindari terjadinya mulititafsir terhadap ketentuan larangan mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan/atau pencemaran nama baik', dilakukan 3 (tiga) perubahan sebagai berikut:[19]
   a. menambahkan penjelasan atas istilah 'mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik'.
   b. menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum.
   c. menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang datur dalam KUHP.
2. Menurunkan ancaman pidana pada penghinaan dan/atau pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi 4 (empat) tahun dan/atau denda dari paling banyak Rp. 1 miliar menjadi paling banyak Rp. 750 juta.

Terhadap ayat (4), disebutkan oleh UU No. 19 Tahun 2016 tentang Perubahan Atas UU NO. 11 Tahun 2008 tentang ITE disebutkan bahwa 'ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan/atau denda paling banyak Rp. 2 miliar menjadi paling banyak Rp. 750 juta.[20]

Pasal 28:

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (SARA).

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".

Pasal 30:

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

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elktronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronbik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang di transmisikan.

Pasal 32:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik.

[19] Indah Mutiara Kami, Fino Yurio Kristo, *Ini 7 Poin Utama Revisi UU ITE Yang Mulai Diberlakukan Hari Ini,* diakses dari https:// m.detik.com pada tanggal 26 Januaru 2023

[20] *Ibid.*

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

Pasal 33:

”Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya”.

Pasal 34:

(1) 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 atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan pasal 33;
   b) sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan pasal 33.

Pasal 35:

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

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 37:

”Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia”.

Tindak pidana sebagaimana disebutkan di atas (Pasal 27 sampai dengan Pasal 37) diancam dengan pidana penjara (maksimumnya berkisar antara 6 (enam) tahun sampai dengan 12 (dua belas) tahun) dan/atau pidana denda (maksimumnya berkisar antara Rp. 600.000.000,00 (enam ratus juta rupiah) sampai dengan Rp.12.000.000.000,00 (dua belas milyar rupiah).

Selain itu terhadap pidana penjara dapat diberikan pemberatan yaitu ditambah dengan sepertiga dari hukuman pokok apabila:

- tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak;
- tindak pidana yang disebutkan dalam Pasal 30 sampai dengan pasal 37 ditujukan terhadap kompuiter dan/atau sistem elektronik serta informasi elektronik dan/atau dokumen elektronik adalah milik pemerintah dan/atau yang digunakan uintk kepentingan publik;
- tindak pidana yang disebutkan dalam pasal 30 sampai dengan Pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta informasi elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, dan otoritas penerbangan.
- tindak pidana yang disebutkan dalam Pasal 27 sampai dengan pasal 37 dilakukan oleh korporasi.

Pasal-pasal yang menyangkut ketentuan pidana diatur dalam Pasal 45 sampai dengan Pasal 52. Dari ketentuan yang terdapat dalam Undang-Undang Tentang Informasi Dan Teknologi Informasi No. 11 Tahun 2008 yang telah diubah dengan UU No. 19 Tahun 2016 ini terlihat bahwa ruang lingkup yang telah dikemukakan ternyata tidak jauh berbeda dengan apa yang telah diatur dalam perundang-undangan di negara lain.

Khusus mengenai *hacking*, diatur secara tersendiri dalam Pasal 32 ayat (1) yang berbunyi : ”Setiap orang dengan sengaja atau tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik”.

Sebenarnya pasal-pasal lain dapat juga dikenakan pasal *hacking* ini, karena *hacking* merupakan *first crime*. Bagaimana dapat mengubah, menghapus atau menambah data komputer apabila dia tidak bisa masuk ke dalam sistem jaringan komputer yang menjadi korban, sedangkan masuk ke dalam sistem jaringan komputer merupakan langkah *hacking* yang kedua setelah sebelumnya melakukan observasi terhadap sistem operasi yang dipakai.

Menurut Barda Nawawi Arief, kebijakan yang ditempuh yang berkaitan dengan kegiatan di *Cyberspace* sebagai berikut:

a. Dalam Buku I (ketentuan Umum) dibuat ketentuan mengenai:
   - Pengertian ’barang’ (pasal 147) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.
   - Pengertian ’anak kunci’ (Pasal 178) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, sinyal yang telah diprogram untuk membuka sesuatu. Maksud dari ’anak kunci’ ini kemungkinan besar adalah *password* atau kode-kode tertentu seperti privat atau *public key infrasturture*.
   - Pengertian’surat’ (Pasal 188) termasuk data tertulis atau tersimpan dalam disket, pita magnetik, media penyimpanan komputer atau penyimpanan data komputer lainnya.
   - Pengertian ’ruang’ (Pasal 189) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu. Maksud dari ’ruang’ ini kemungkinan termasuk pula ’dunia maya’ atau ’mayantara’ atau *’cyberspace’* atau *’virtual reality’.*
   - Pengertian ’masuk’ (Pasal 190) termasuk mengakses komputer atau masuk ke dalam sistem komputer. Maksud pengertian ’masuk’ dalam pasal ini bukanlah masuk ke dalam komputer atau sistem komputer (karena seperangkat atau sebuah komputer atau beberapa komputer yang terhubung seperti LAN sudah merupakan sistem), melainkan masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke komputer yang termasuk dalam pengertian situs atau website yang di dalamnya berupa server dan komputer yang termasuk dalam pengelolaan situs. Ada dua (2) pengertian ’masuk’ yaitu: masuk ke ’internet’ dan masuk ke ’situs’.
   - Pengertian ’jaringan telepon’ (Pasal 191) termasuk ajringaan komputer atau sistem komunikasi komputer.

b. Dalam Buku II:
   Dengan dibuatnya ketentuan seperti di atas, maka konsep tidak atau belum membuat delik khusus untuk *cybercrime atau computer related crime.* Konsep juga mengubah perumusan delik atau menambah delik-delik baru yang berkaitan dengan kemajuan, teknologi, dengan harapan dapat menajring kasus-kasus *cyber crime,* antara lain:
   - Menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis (Pasal 263).
   - Memasang alat bantu teknis untuk tujuan mendengar atau merekam pembicaraan (Pasal 264).
   - Merekam (Memiliki atau menyiarkan) gambar dengan alat bantu teknis di ruangan tidak untuk umum (Pasal 266).
   - Merusak atau membuat tidak dapat dipakai bangunan untuk sarana atau prasarana pelayanan umum, seperti bangunan telekomunikasi atau komunikasi lewat satelit atau komunikasi jarak jauh (Pasal 546).
   - Pencucian uang atau *money laundering* (Pasal 641- Pasal 642).[21]

Dari uraian di atas, dapat diketahui bahwa ada usaha yang harus dilakukan oleh pemerintah dalam menanggulangi *cybercrime* dengan menggunakan sarana penal, yaitu dengan membuat Undang-Undang mengenai Informasi Dan Traksaksi Elektronik No. 11 Tahun 2008 yang kemudian diubah dengan UU No. 19 Tahun 2016 dan upaya memperluas pengaturan-pengaturan *cyberspace* dalam Kitab Undang-Undang Hukum Pidana Nasional dengan memperluas beberapa pengertian yang berkaitan dengan kegiatan di *cyberspace.*

Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus *cybercrime* adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan adanya UU ITE ini diharapkan dapat melindungi masyarakat pengguna teknologi informasi di Indonesia, hal ini penting mengingat jumlah pengguna teknologi internet yang semakin meningkat dari tahun ke tahun. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan suatu perbuatan tindak pidana, kemajuan teknologi ini juga mempengaruhi gaya hidup dan pola pikir manusia faktanya saat ini banyak terjadi kejahatan dengan menggunakan teknologi informasi. Fenomena *cybercrime* yang berkembang dengan pesat yang tidak mengenal batas teritorial ini memang harus diwaspadai karena kejahatan ini

[21] Barda Nawawi Arief**,** *Antisipasi Penanggulangan Cybercrime Dengan Hukum Pidana,* Makalah pada Seminar Nasional *Cyberlaw*, diselenggarakan oleh STH Bandung, 9 April 2001, hlm. 13-14.

agak berbeda dengan kejahatan lain pada umumnya.[22]

Pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia. Di dalam ketentuan Pasal 4 ayat (2) UU ITE disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.[23]

Penyalahgunaan teknologi informasi ini yang dapat merugikan orang lain, bangsa dan negara yang menggunakan sarana komputer yang memiliki fasilitas internet yang dilakukan oleh hacker atau sekelompok *cracker* dari rumah atau tempat tertentu tanpa diketahui oleh pihak korban yang dapat menimbulkan kerugian moril, materil maupun waktu akibat dari perusakan data yang dilakukan oleh *hacker*. Untuk mengatasi kejahatan *cybercrime* dibutuhkan aparat penegak hukum yang memahami dan menguasai teknologi, kendala yang dihadapi oleh korban adalah dikarnakan ketidaktahuan, pengetahuan komputer dan internet sehingga apabila dirugikan tidak dapat melaporkaan segala peristiwa pidana yang dialami tentunya ini menjadi permasalahan kita bersama.[24]

Asas dan tujuan undang-undang ini adalah pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Jadi dapat diartikan bahwa pengunaan teknologi informasi dan Transaksi elektronik diharapkan dijamin dengan kepastian hukum, memiliki manfaat, penuh kehati-hatian, beritikad baik, dan adanya kebebasan memilih teknologi dan netral.

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang diharapkan mampu untuk menjawab semua permasalahan hukum terhadap perkembangan global teknologi serta antisipatif terhadap semua permasalahan yang ada, termasuk dampak negatif penyalahgunaan internet yang pada akhirnya akan menimbulkan kerugian bagi penggunanya. Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain :[25]

1. Kitab Undang-Undang Hukum Pidana
2. Undang-Undang Nomor 19 tahun 2016 tentang ITE
3. Undang-Undang Nomor 44 tahun 2008 tentang Pornografi
4. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.
5. Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat.
6. Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen.
7. Undang-Undang Nomor 28 tahun 2014 tentang Hak Cipta.
8. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
9. Undang-Undang Nomor 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang
10. Undang-Undang Nomor 9 Tahun 2013 tentang Pemberantasan Terorisme

Dalam menjaga dan melindungi masyarakat pengguna teknologi dibutuhkan kerjasama dan keseriusan semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur *cybercrime* diharapkan dapat melindungi dan memberikan rasa aman bagi mereka yang menggunakan teknologi sebagai wadah untuk melalukan transaksi maupun melakukan kegiatan ekonomi. Dalam melakukan penindakan bagi mereka yang menyalahgunakan perkembangan teknologi dibutuhkan sumberdaya manusia yang berkualitas yang memiliki kemampuan dan keahlian dibidang teknologi. Dalam penegakan hukum setidaknya dipengaruhi beberapa faktor yakni aturan hukum itu sendiri atau undang-undang, aparat pelaksana dari aturan tersebut yakni aparat penegak hukum dan budaya hukum itu sendiri yakni masyarakat itu sendiri yang menjadi sasaran dari undang-undang.[26]

Dengan adanya undang-undang ITE tersebut diharapkan dapat memberikan rasa aman dan

[22] Josua Sitompul, "*Cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana*", PT. Tatanusa, Jakarta, 2012, Hal. 39
[23] *Ibid*, Hlm. 39
[24] *Ibid*
[25] Dheny Wahyudi, "*Perlindungan Hukum Terhadap Korban Kejahatan Cybercrime di Indonesia*", Jurnal Ilmu Hukum, Volume 3, Nomor 5, April 2017, Hlm. 104
[26] *Ibid*

dapat melindungi bagi mereka yang menggunakan teknologi. Disamping itu, dalam keadaan tertentu dan membahayakan bagi mereka yang menjadi korban kejahatan teknologi juga berhak mendapatkan perlindungan hukum hal ini tercantum dalam Undang-undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban.

Ada beberapa alternatif pemecahan dalam rangka pencegahaan dan penanggulangan kejahatan dengan sarana penal berupa peraturan perundang-undangan. Alternatif-alternatif tersebut sebagai berikut:

a. Jika yang hendak dibuat adalah *cyberlaw* sebagai *'umbrella provision'*, maka langkah yang harus diambil adalah membuat kertentuan *cybercrime* yang dapat mencakup semua kegiatan di *cyberspace*. Mengingat ketentuan ini merupakaan ketentuan pidana khusus, maka aturan main yang bersangkutan dengan prinsip atau asas-asas umum harus diatur secara tersendiri. Jika ketentuan *cybercrime* tidak mengatur secara tersendiri mengenai prinsip atau asas-asas umum itu, maka apakah ketentuan umum dalam Buku I KUHP dapat diberlakukan kepadanya, mengingat sifat yang berbeda dari *virtual reality dan real life.* Ini berarti ada pemisahan antara ketentuan pidana yang berlaku untuk kegiatan di *cyberspace* atau dunia maya (RUU-KUHP) dan ketentuan pidana yang mengatur kegiatan di kehidupan nyata (KUHP yang seperti sekarang ada).
b. Jika yang ingin dikembangkan adalah Kitab Undang-Undang Hukum Pidana (KUHP)-nya (yang sekarang dilakukan dengan penafsiran) atau dalam KUHP mendatang dengan memperluas penafsiran (*interpretatie ekstensive*) yang dapat menajngkau kegiatan di *cyberspace*, maka ketentuan pidana di *cyberlaw* atau peraturan tersedndiri mengenai *cybercrime* tidak diperlukan, karena KUHP merupakan kodifikasi dari hukum pidana. Jika model ini yang diambil/dianut, maka harus dikembangkan langkah-langkah untuk menyesuaikan dengan perkembangan *cyberspace* yang begitu cepat, yaitu dengan melakukan amandemen. Dengan demikian, antara dunia nyata (*real life*) dan dunia maya hanya ada satu (1) ketentuan pidana yang mengatur kegiatan di kedua dunia tersebut.

Membuat regulasi terhadap suatu aktivitas yang sangat kompleks seperti *hacking*, apalagi dalam kaitannya dengan teknologi informasi (dimana Indonesia dalam hal teknisnya masih agak tertinggal) bukanlah suatu pekerjaaan yang mudah. Untuk mengadakan perubahan hukum pidana yang ada, orang tidak boleh bertindak begitu saja tanpa ada penelitian yang cukup mendalam sebelumnya. Untuk itu, diperlukan fakta-fakta dan data statistik yang dapat menajdi dasar penentuan sesuatu keputusan kehendak dari pembentuk Undang-Undang yang berupa suatu peraturan.[27]

Hal senada juga diungkapkan oleh Muladi dalam konteks pembahasan mengenai pengaturan *cybercrime*. Muladi menegaskan adanya persyaratan *academic draft* yang secara komprehensif dapat meyakinkan pengundang-undangan tentang betapa pentingnya proses tersebut atas dasar kebutuhan hukum yang berkaitan dengan substansinya.[28]

Selain adanya pengkajian terhadap masalah yang hendak di kriminalisasi (yang hasilnya berupa *academic draft*), persyaratan lain yang perlu diperhatikan adalah kerugian atau korban, baik aktuil maupun potensial yang signifikan dengan perbuatan tersebut, tidak boleh bersifat *ad hoc,* ketentuan hukum pidana harus dapat di operasionalisasikan (*enforceable*) dan adanya keyakinan bahwa tidak ada sarana lain yang dapat mengatasinya (*ultima ratio principle*). Syarat terakhir sangat penting untuk menghindarkan adanya kondisi yang disebut kriminalisasi yang berlebihan (*over criminalization*) atau inflasi pengaturan yang mengakibatkan turunnya nilai hukum pidana di masyarakat, sehingga bersifat *counter productive*. Hal ini antara lain dalam bentuk terhambatnya kreatifitas pengembangan teknologi informatika. Belum lagi persyaratan teknis, yaitu keharusan untuk memenuhi 'asas *lex certa'* bahwa perumusan harus jelas sehingga dapat dipercaya.[29]

PENUTUP

A. Kesimpulan

1. Perkembangan teknologi yang semakin cepat dan kemajuan ilmu pengetahuan tidak dapat disangkal mengakibatkan munculnya kejahatan-kejahatan atau tindak pidana yang berkaitan dengan kecanggihan teknologi atau yang dikenal dengan kejahatan/tindak pidana *cyber crime,* dimana bentuk-bentuknya begitu banyak dan beragam seperti *identity theft*, kejahatan *phishing*, kejahatan *carding*, serangan *ransomware*, penipuan *online*, SIM *swap*, peretasan situs dan *email*, kejahatan

[27] Sudarto, *Op-Cit*, hlm-97.

[28] Muladi, *Prospek Pengaturan Cybercrime di Indonesia*, Makalah pada Seminar Nasional *Money Laudering* dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana Universitas Surabaya, 24 Pebruari 2001, hlm-1.

[29] *Ibid.*

skimming, OTP *Fraud*, pemalsuan data atau data *forgery*, kejahatan konten ilegal, teroris dunia maya atau *cyber terorism*, mata-mata atau *cyber espionage*, dan menjiplak situs orang lain. Dari beragam bentuk *cyber crime* ini yang sering terjadi adalah bentuk akses ilegal (*carding*), *phishing*, penipuan OTP, kejahatan konten ilegal, membajak sistem komputer dan *cyber terorism*.

2. Upaya penanggulangan *cybercrime* dengan sarana penal, yaitu selain sudah diatur dalam pasal-pasal yang ada dalam KUHP seperti Pasal 362 tentang Pencurian, Pasal 378 tentang Penipuan dan Pasal 263 tentang Pemalsuan identitas dengan ancman hukuman yang ada, juga dengan dibelakukannya UU No. 11 Tahun 2008 yang dirobah dengan UU No. 19 Tahun 2016 tentang ITE khususnya dalam Pasal 27 sampai dengan Pasal 37 tentang Perbuatan yang dilarang dan dalam Pasal 45 sampai dengan Pasal 52 tentang ancaman penjara dengan mengenakan ancaman hukuman penjara paling berat 12 (dua belas) tahun dan hukuman denda paling banyak Rp. 2.000.000.000,00 (dua milyar rupiah).

B. Saran

1. Pemerintah perlu untuk men-sosialisasikan tentang bentuk-bentuk kejahatan *cyber crime* serta dampak yang diakibatkan sampai ke masyarakat pedesaan karena penggunaan alat-alat teknologi sudah mencapai ke masyarakat pedesaan dan hampir sebagian besar masyarakat khususnya orang muda sudah tahu menggunakan hand phone yang merupakan alat dalam saling berkomunikasi, bertukar informasi bahkan melakukan transaksi. Sosialisasi perlu dilakukan agar masyarakat semakin menyadari dan mengetahui teknik-teknik yang digunakan oleh *hacker* dalam hal ini pelaku kejahatan *cyber crime* agar masyarakat semakin waspada dalam menggunakan internet dalam kehidupan sehari-hari.
2. Perbuatan pidana atau tindak pidana mayantara atau *cybercrime* harus dihukum dengan ancaman hukuman yang berat dan juga harus disertai dengan ancaman denda yang besar. Harus diberikan ancaman hukuman kumulatif dalam ancaman pidana pokoknya yaitu pidana penjara sekaligus denda agar supaya pelaku benar-benar jera untuk melakukannya kembali. Selain itu pemerintah perlu lebih mengembangkan dan meningkatkan lagi SDM serta teknologi tim khusus kejahatan *cyber* untuk melacak pelaku kejahatan *cyber crime* agar para pelaku kejahatan tidak lagi leluasa dalam melaksanakan kejahatannya.

DAFTAR PUSTAKA

Arief Nawawi Barda. Bunga Rampai Kebijakan Hukum Pidana : Perkembangan Penyusunan Konsep KUHP Baru. Jakarta. Kencana Prenada Media Group. 2008

Arief, Barda Nawawi., *Antisipasi Penanggulangan Cyber Crime Dengan Hukum Pidana,* Makalah pada Seminar Nasional ”Cyber Law”, STHB, Bandung, 9 April 2000.

Budhijanto, Danrivanto., *Aspek-Aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce)*, Makalah pada Seminar Aspek Hukum Transaksi Perdagangan via Internet, FH UNPAD, Bandung, 22 Juli 2000.Hukum di Indoensia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 Pebruari 2001.

Komar, Kantaatmadja, Mieke., *Menyongsong Penyusunan Peeraturan Perundang-undangan Telematika (Cyberlaw)*, Makalah pada Seminar Nasional Tentang Aspek Hukum Transaksi Perdagangan via Internet di Indonesia, diselenggarakan oleh SEMA FH UNPAD, Bandung, 22 Juli 2000.

Latifulhayat, Atip., *Cyberlaw dan Urgensinya Bag Indonesia*, Makalah pada Seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000

Mahendra, Yusril Ihza., *Regulasi Cyberspace di Indonesia*, Makalah pada Seminar tentang Cyber Law, diselenggarakan oleh yayasan Cipta Bangsa, bndung, 22 Juli 2000.

Mansur Arief M Didik, Gultom Elisatris. Cyber Law Aspek Hukum Teknologi Informasi. PT Refika Aditama. Bandung. 2005

Moeljatno, *Azas-Azas Hukum Pidana,* Bina Aksara, Jakarta, 1983.

Muladi, Arief Nawawi Barda.Teori-Teori dan Kebijakan Hukum Pidana. Bandung. Alumni. 2010

Muladi., *Prospek Pengaturan Cybercrime di Indonesia*, Makalah pada Seminar
Nasional Money laundering dan Cybercrime dalam Perspektif Penegakan

Prodjodikoro Wirjono, *Asas-asas Hukum Pidana di Indonesia,* edisi ketiga, Refika Aditama, Bandung, 2003

Remellink J. Pengantar Hukum Pidana Materiil 1.Sungging.Yogyakarta.2014

Sianturi S.R, *Azas-Azas Hukum Pidana di Indonesia dan Penerapannya*, Alumni AHM-PTHM,Jakarta, 1989.

Sudarto., *Hukum dan Hukum Pidana*, Alumni, Bandung, 1986.

Wahyudi Dheny.Perlindungan Hukum Terhadap Korban Kejahatan.Cybercrime di Indonesia. Jurnal Ilmu Hukum. Volume 3.Nomor 5. April 2017

Walker, Nigel dalam Muladi., *Proyeksi Hukum Pidana Materil Indonesia di masa Mendatang*, Pidato Pengukuhan Guru Besar Univ. Diponegoro, Semarang, 1990.

Sumber internet

Contoh Kasus Cybercrime Di Indonesia Dan UU ITE terkait, diakses dari https://edybillstephen.ilearning.me pada tanggal 20 Desember 2022.

Feradhita nkd, *Mengetahui 3 contoh Kasus Cyber crime di Indonesia*, diakses dari https://www.logique.co.ic pada tanggal 20 Desember 2022.

Pengertian Penanggulangan diakses dari https://kbbi.web.id pada tanggal 23 April 2020.

Upaya Penanggulangan Kejahatan diakses dari https://raypratama.blogspot.com pada tanggal 23 April 2020.

14 Jenis Cyber crime, Kejahatan Internet Yang Merugikan, 21 November 2022, diakses dari https://www.cermati.com pada tanggal 28 Juli 2023.

Undang-Undang

Kitab Undang-Undang Hukum Pidana

UU No. 11 Tahun 2008 yang dirubah dengan UU No. 19 Tahun 2016 tentang *Informasi dan Transaksi Elektronik*