KEJAHATAN SIBER YANG MENJADI KEKOSONGAN HUKUM

Cheny Berlian

Universitas Muhammadiyah Riau, Indonesia, chenyberlian@umri.ac.id

Abstract

In today's technological era, there are more and more crimes occurring in the field technology or better known as Cyber Crime, where these crimes are always growing every year. The number of Cyber Crime cases has certainly disturbed the community, resulting in the Creation Of Law Number 11 Of 2008 Concerning Electronic Information And Transactions And Law Number 19 Of 2016 Concerning Amendments To Law Number 11 Of 2008 Concerning Electronic Information AndTransactions.However, not all crimes that occur can be protected by the ITE Law, there are many cyber crime cases where there is no legal protection so this creates a legal vacuum.

Keywords : Cyber Crime, UU ITE

Abstrak

Pada era teknologi sekarang ini, semakin banyak terjadinya kejahatan dalam bidang teknologi atau yang lebih dikenal sebagai *Cyber Crime*, yang mana kejahatan-kejahatan tersebut selalu berkembang setiap tahunnya. Banyaknya kasus-kasus *Cyber Crime* tersebut tentu meresahkan masyrakat, sehingga diciptkannya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun tidak semua kejahatan yang terjadi dapat dilindungi oleh

Undang-Undang ITE tersebut, ada banyak kasus-kasus kejahatan siber yang tidak ada perlindungan hukumnya sehingga hal ini membuat adanya kekosongan hukum.

Kata kunci : Kejahatan Siber, UU ITE

PENDAHULUAN

Kemunculan teknologi digital dalam dunia informasi dan komunikasi mempengaruhi seluruh aspek kehidupan manusia. Teknologi internet menyediakan berbagai kemudahan dalam mencari dan memberikan informasi kepada masyarakat. Pola kehidupan manusia saat ini telah banyak mengalami perubahan, sejak hadirnya teknologi internet, bumi seakan menjadi desa kecil yang tidak pernah tidur, semua jenis kegiatan dapat difasilitasi oleh teknologi internet.[1] Pemanfaatan media internet pada masa sekarang ini memberikan dampak yang cukup luas bagi hampir sebagian besar aspek kehidupan manusia dimana internet menjadi media penyampaian serta pertukaran informasi, disamping juga sebagai sarana atau media baru dalam melakukan interaksi sosial yang biasanya terjadi secara tidak langsung dan bersifat *borderless* (tanpa mengenal batas wilayah).

Umumnya suatu masyarakat yang mengalami perubahan akibat kemajuan teknologi, banyak melahirkan masalah-masalah social. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi yang tidak lagi dapat

[1] Budi Sutedjo Dharma Oetomo, *E-education : Konsep, Teknologi dan Aplikasi Internet Pendidikan*, Andi, Yogyakarta, 2007, hlm. 11.

diterima.[2] Dampak negatif terjadi akibat pengaruh penggunaan media *internet* dalam kehidupan masyarakat dewasa ini. Melalui media *internet* beberapa jenis tindak pidana semakin mudah untuk dilakukan seperti, tindak pidana pencemaran nama baik, pornografi, perjudian, pembobolan rekening, perusakan jaringan *cyber Hacking)*, penyerangan melalui virus *(virus attack)* dan sebagainya.

Di Indonesia sendiri terdapat UU ITE yang merupakan *cyberlaw* pertama yang dimiliki Indonesia dan menjadi landasan hukum bagi anggota masyarakat dalam beraktivitas di dunia *cyber*.[3] Pengaturan tindak pidana *cyber* dalam peraturan perundang-undangan Indonesia seperti dalam UU ITE telah melengkapi hukum pidana materiil Indonesia yang mengatur berbagai tindak pidana yang berkembang seiring dengan pertumbuhan teknologi informasi dan komunikasi.[4]

Pengaturan tindak pidana *cyber* dalam UU ITE dan peraturan perundang-undangan lainnya mengandung implikasi adanya perlindungan hukum terhadap kepentingan-kepentingan hukum masyarakat, khususnya berupa data komputer atau data elektronik, dokumen elektronik, informasi elektronik, dan sistem komputer atau sistem elektronik yang dilindungi dan tidak bersifat publik, baik milik pribadi maupun negara serta kepentingan hukum lainnya seperti, harta kekayaan, kehormatan dan kesusilaan, keamanan negara, dan lain-lain.[5]

[2] Horton, Paul B dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984, hlm.237.

[3] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Bandung, PT Refika Aditama, 2012, hlm.
213.

[4] *Ibid.*

[5] *Ibid*., hlm. 214.

Ada banyak jenis *Cybercrime* yang ada di Indonesia yaitu *Hacking, Cracking, Defacing, Carding, Fraud, Spamming, Cyberpornography,* dan *Onlne Gambling*. Selain itu, permasalahan mengenai kebebasan dalam menggunakan media sosial sering kali menimbulkan berbagai penyalahgunaan. Salah satu penyalahgunaan media sosial yang akhir- akhir ini marak ditemui adalah *internet troll*. *Trolling* diartikan sebagai tindakan seseorang yang memposting tulisan atau pesan menghasut dan tidak relevan dengan topik yang dibicarakan di komunitas online seperti forum, *chatting*, dan bahkan blog. Dengan maksud atau tujuannya adalah memprovokasi dan memancing emosi para pengguna internet lainnya agar jalannya diskusi yang tengah berlangsung menjadi kacau.

Dalam dunia internet, pelaku *trolling* ini disebut *troller*. *Troller* dapat diartikan sebagai *provocateur* alias provokator. Contoh kasus internet troll ini sering kali berbentuk *cyberbullying* yang membuat seseorang menjadi tertekan, akibatnya para korban kerap menggambil keputusan bunuh diri. Contohnya saja artis Korea yaitu Sulli di mana banyak komentar negatif mengenai dirinya bertebaran di media sosial, sehingga membuat psikologis nya menjadi terganggu, akibatnya artis Korea Sulli tersebut mengambil keputusan bunuh diri. Dikutip dari Jurnal Komunikasi Malaysian Journal

Selanjutnya, dalam bidang *E-Commerce* kecurangan dapat dilakukan oleh seluruh pihak yang terlibat dalam melakukan transaksi, yaitu penjual, pembeli, maupun karyawan pada perusahaan *E-*

Commerce. Beberapa kasus terkait dugaan terjadinya praktik kecurangan pada *E-Commerce* di Indonesia adalah dalam penyelenggaraan *Flash Sale* oleh *Platrform Market Place* yang menyebabkan banyak konsumen tidak dapat memperoleh barang yang dijual dengan harga murah pada saat *flash sale* berlangsung, dan menyebabkan konsumen dirugikan.

Seperti permasalahan internet troll di Indonesia belum ada aturan khusus yang mengatur bagaimana penegakan hukum terhadap pelaku *trolling* di media sosial. Sehingga, para pelaku dapat dengan bebas mengincar pengguna media social bahkan cenderung merajarela pada saat ini. Berbeda dengan Negara lain yang sudah mulai fokus terhadap penegakan hukum kepada *troller*. Belum lama ini, Inggris membuat aturan hukum baru yang khusus mengincar para troll di Internet. Dengan aturan tersebut troll internet yang membuat tagar menghina atau memposting foto rekayasa (meme) untuk mempermalukan orang lain bisa dihadapkan pada tuntutan hukum. Aturan tersebut juga menyatakan, menghasut orang untuk melecehkan orang lain secara online dapat mengakibatkan tuntutan pengadilan. Hal ini berarti bahwa pelakunya akan diadili dengan cara yang sama seperti layaknya pelaku yang dilakukan secara nyata tanpa melalui media sosial.

Cyberbullying adalah suatu bentuk bullying yang terjadi online, melalui media sosial, gaming atau ruang ngobrol (chat room). Berbeda dengan bullying tradisional, karena *Cyberbullying* terjadi 24 jam/hari, 7 hari/minggu, dan mencapai korbannya dimanapun dia berada termasuk di

rumah.[6] *Cyberbullying* memiliki banyak bentuk, antara lain[7] :

a. Pelecehan/ provokasi emosi (*harassment/ trolling*), adalah mengirimkan pesan bersifat mengancam atau menyerang, berbagi foto atau video aib/vulgar, atau memposting pesan yang mengancam atau memancing amarah pada situs jejaring sosial.
b. Fitnah (*denigration*), adalah informasi palsu, salah,berupa gosip yang menyebar.
c. Penyulut kemarahan (*flaming*), menggunakan bahasa ekstrim untuk memancing perkelahian.
d. Mencuri identitas seseorang atau membajak situs seseorang (*hacking*).
e. Pengecualian (*exclusion*), meninggalkan seseorang secara sengaja.
f. Mengirimkan gambar atau memaksa seseorang untuk mengirim gambar seksual.

Mengutip dari Jurnal Komunikasi Malaysian Journal of Communication yang menyatakan[8] :

> "mengikut akhbar The Sun di United Kingdom pada 24 Ogos 2017, menjelaskan bahawa "troll" ini adalah slanga yang merujuk kepada seseorang yang secara sengaja memulakan pertelingkahan di Internet bagi tujuan provokasi bagi menarik reaksi daripada individual atau berkumpulan terhadap provokasi tersebut. hanya boleh jadi dimulakan dengan perdebatan sihat, namun kemudian menjadi pertelingkahan di ruang maya yang diviralkan. Di dalam politik, trolling ini yang boleh dibuat dalam bentuk satira juga digunakan bagi mendapatkan reaksi politik di pihak pemerintah mahupun pembangkang. Di dalam dunia

[6] Fahmi Anwar, *Perubahan dan Permasalahan Media Sosial* , Jurnal Muara Ilmu Sosial, Humaniora, dan Seni Vol. 1, No. 1, April 2017: hlm 141.

[7] *Ibid.*, hlm. 142.

[8] Raja Nur Afiqah Zulkifli, dkk., *Satira Politik: Analisis Internet Trolling di Malaysia* , Jurnal Komunikasi Malaysian Journal of Communication , Jilid 34(2) 2018: 223-242 , hlm. 225

> tanpa sempadan dan kawalan, Internet telah dijadikan medan untuk ramai pengguna Internet untuk melancarkan trolling ke atas ahli dan badan politik yang mereka sukai dan juga benci bagi menyampaikan maksud dan idea politik tertentu"

Trolling politik di Malaysia lazimnya dapat diakses melalui pelbagai aplikasi terutama sekali Facebook. Aktiviti memuatnaik ini menjadi semakin rancak apabila terdapat laman Facebook khusus tentang aktiviti ini. Proses penularan bahan trolling tersebut menjadi mudah dan pantas dengan terdapatnya butang "perkongsian" yang tersedia dalam aplikasi Facebook tersebut.[9]

Permasalahan selanjutnya adalah terkait perlindungan konsumen dalam melakukan transaksi *E-commerce* juga masih kurang efektif dikarenakan pengaturan hukum di Indonesia masih terdapat celah bagi para pelaku untuk melakukan kecurangan. Kasus *flash sale* merupakan salah kasus yang membuat konsumen dirugikan dan seringkali para konsumen mengalami kebingungan untuk melakukan suatu upaya terhadap kecurangan yang menimpa mereka. Perbandingan pengaturan terkait dengan *e-commerce* dan kecurangan dapat kita lihat di beberapa pengaturan hukum baik dari hukum internasional maupun nasional. Peraturan perundang-undangan mengenai *e-commerce* masih membutuhkan banyak perbaikan dan perlunya memiliki peraturan perundang-undangan secara khusus mengatur secara spesifik mengenai transaksi perdagangan elektronik, baik dari segi proses, perlindungan konsumen, maupun pengaturan mengenai tindak kecurangan yang dapat dilakukan pada *e-commerce*.

[9] *Ibid.*, hlm. 226.

Kondisi peraturan perundang-undangan di Indonesia mengenai *e-commerce* masih tersebar di beberapa undang-undang dan terkendala adanya banyak celah yang dijadikan peluang bagi para pelaku kejahatan untuk memperoleh keuntungan tanpa memikirkan kerugian yang diderita konsumen.

Kecurangan-kecurangan yang dilakukan pelaku usaha sering dijadikan peluang untuk memperoleh keuntungan tanpa memikirkan kerugian yang diderita konsumen. *United Nations Commision on International Trade Law* (UNCITRAL) *Mode Law on Electronic Commerce with Guide to Enactment 1996* merupakan pedoman bagi negara-negara untuk membentuk peraturan di negaranya masing. Di Indonesia pengaturan mengenai perlindungan konsumen pada transaksi *e-commerce* terdapat pada Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Belum terdapat pengaturan secara spesifik pada tindakan curang di transaksi *e-commerce* menjadikan celah dan seringkali menimbulkan kerugian dan ketidakpastian hukum pada konsumen.

Kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dalam buku Barda nawawi arief, adalah kualifikasi (*cybercrime*) menurut *convention on cybercrime* 2001 di Budapest Hongaria, yaitu: *illegal access*: yaitu sengaja

memasuki atau mengakses sistem komputer tanpa hak. Sedangkan kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dalam buku barda nawawi arief, adalah kualifikasi (*cybercrime*) menurut *Convention on cybercrime* 2001 di Budapest Hongaria, yaitu[10] :

a. *Illegal interception*: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diamdiam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.
b. *Data interference*: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
c. *System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.
d. *Misuse of devices*: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code).
e. *Computer related forgery*: pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud

[10] Barda Nawawi Arief, Tindak Pidana Mayantara, *Perkembangan Kajian Cybercrime di Indonesia*, RajaGrafindo Persada, Jakarta, 2006.

digunakan sebagai data autentik)

f. *Computer related fraud* penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain);
g. *Content-related offences*: delik-delik yang berhubungan dengan pornografi anak (child pornography);
h. *Offences related to infringements of copyright and related rights*: delik-delik. Yang terkait dengan pelanggaran hak cipta.

Selanjutnya, dikutip dari *Southeast Asia Freedom of Expression Network* (SAFEnet) merupakan jaringan pembela hak-hak digital di Asia Tenggara pada tulisan "Bangkitnya Otoritarian Digital Laporan Situasi Hak-hak Digital Indonesia 2019", SAFEnet menemukan bahwa kekerasan terjadi lintas dan multiplatform digital. Pelaku memanfaatkan berbagai teknologi digital untuk bisa berkomunikasi dengan korban, dari aplikasi kencan (*dating apps*), aplikasi percakapan (*chatting apps*), seperti WhatsApp, Line; aplikasi bersurat (e-mail); ataupun memanfaatkan fitur pesan langsung (*direct message*) di media

sosial atau bahkan Identitas sengaja disamarkan.[11]

Selama platform-platform digital tersebut memiliki fitur interaktif antar pengguna, maka dia sudah berpotensi menjadi ruang kekerasan digital. Pemanfaatan berbagai teknologi komunikasi digital ini memungkinkan korban dan pelaku berada di lokasi berbeda dengan jarak jauh, seperti beda kota, beda provinsi, bahkan beda negara. Saat mendampingi aduan kasus KBGS sepanjang 2019, SAFEnet juga melakukan konsultasi tatap muka langsung dengan korban (23%). Meskipun demikian mayoritas pendampingan dilakukan secara daring karena domisili korban ada di berbagai tempat. Tidak semua aduan yang tercatat berujung pada pelaporan ke polisi, karena korban memilih untuk tidak sampai pada hal tersebut. Alasan-alasan yang dikemukakan termasuk tidak ingin ketahuan orang tua, proses yang panjang, ketakutan atas *victim blaming* atau dikriminalisasi dengan UU ITE, biaya, dan lain-lain. Dari kasus yang turut didampingi SAFEnet sampai di tahap pelaporan ke polisi dilakukan dengan berkoordinasi bersama lembaga bantuan hukum, seperti LBH APIK Jakarta, LBH Jakarta, dan LBH Bandung.[12]

Penelitian hukum merupakan kegiatan ilmiah yang didasarkan pada metode, sistematika, dan pemikiran tertentu, yang bertujuan untuk mempelajari satu atau beberapa gejala

[11] Bangkitnya *Otoritarian Digital Laporan Situasi Hak-hak Digital Indonesia 2019*, Southeast Asia Freedom of Expression Network (SAFEnet), Juli 2020, hlm. 30.

[12] *Ibid.*

hukum tertentu, dengan jalan menganalisisnya.[13]

1. Spesisifikasi Penelitian

Penelitian ini bersifat deskriptif analitis, yaitu bersifat pemaparan dan bertujuan untuk memperoleh gambaran (deskriptif) lengkap tentang keadaan hukum yang berlaku di tempat tertentu dan pada saat tertentu yang terjadi dalam masyarakat.[14], pada penelitian ini khususnya mengkaji mengenai mengenai Kejahatan Siber yang Menjadi Kekosongan Hukum

2. Metode Pendekatan

Penelitian ini merupakan penelitian hukum normatif yang didasarkan pada data sekunder dengan metode pendekatan undang- undang, pendekatan komparatif, dan pendekatan konseptual yang difokuskan untuk mengkaji Kebijakan Formulasi terhadap Kejahatan Siber berdasarkan Asas Legalitas.. Analisis data yang digunakan dalam penelitian ini adalah analisis kualitati deskriptif dan preskriptif. Fokus kajian yuridis normatif adalah inventarisasi hukum positif, asas-asas dan doktrin hukum, penemuan hukum dalam perkara *in concreto*, sistematik hukum, taraf sinkronisasi hukum, perbandingan hukum, dan sejarah hukum.[15] Pendekatan ini dapat dilakukan melalui studi kepustakaan (*library research*) dengan mengutamakan data sekunder, terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier terkait dengan Hukum Siber.

3. Tahapan Penelitian

[13] Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, PT Citra Aditya Bakti, Bandung, 2004, hlm. 52.

[14] *Ibid*., hlm. 115.

[15] Bambang Sunggono, dalam *Ibid*., hlm. 52.

a. Penelitian Kepustakaan, yaitu penelitian hukum yang dilakukan dengan cara mengkaji bahan pustaka atau data sekunder.[16] Data sekunder tersebut terdiri dari :

1) Bahan hukum primer yaitu bahan-bahan hukum yang mengikat yang terdiri dari :

a) Undang-Undang Dasar 1945

b) *United Nations Commision on International Trade Law (UNCITRAL) Mode Law on Electronic Commerce with Guide to Enactment 1996*

c) Kitab Undang-Undang Hukum Pidana

d) *Law of Malaysia At 758 Electronic Commerce Act* 2006

e) Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

2) Bahan hukum sekunder, yaitu bahan yang memberikan penjelasan mengenai bahan hukum primer, seperti literatur, buku-buku penunjang, disertai jurnal-jurnal hukum terkait dengan permasalahan yang peneliti angkat yaitu tentang Kebijakan Formulasi terhadap Kejahatan Siber berdasarkan Asas Legalitas.

3) Bahan hukum tersier, yaitu bahan-bahan yang memberi petunjuk terhadap bahan hukum primer dan bahan sekunder, yang lebih dikenal dengan nama bahan acuan bidang hukum atau rujukan bidang hukum.[17]

b. Penelitian Lapangan

[16] Soerjono Soekanto, *Penelitian Hukum Normatif Suatu Pengantar*, Rajawali Press, Jakarta, 2006, hlm. 14.

[17] *Ibid..*, hlm. 115.

Penelitian lapangan yang dilakukan oleh peneliti adalah kegiatan mengumpulkan dan meneliti data primer yang diperoleh melalui wawancara secara langsung dari narasumber yang ahli dalam bidang siber.

4. Pengumpulan dan Pengolahan Data

Pengumpulan data dilakukan dengan studi pustaka yang meliputi sumber primer, yaitu perundang-undangan yang relevan dengan permasalahan. Sumber sekunder, yaitu buku-buku literatur ilmu hukum beserta tulisan-tulisan hukum lainnya yang relevan dengan permasalahan.[18] Studi pustaka dilakukan melalui tahap-tahap identifikasi pustaka sumber data, identifikasi bahan hukum yang diperlukan, dan inventarisasi bahan hukum (data) yang diperlukan tersebut. Data yang terkumpul kemudian diolah melalui tahap pemeriksaan (*editing*), penandaan (*coding*), penyusunan (*reconstructing*), sistematisasi berdasarkan pokok bahasan dan subpokok bahasan yang di identifikasi dari rumusan masalah (*systematizing*), yang berkaitan dengan pokok bahasan yang diteliti yaitu Kebijakan Formulasi terhadap Kejahatan Siber berdasarkan Asas Legalitas.

5. Metode Analisis Data

Hasil pengolahan data selanjutnya dianalisis dengan menggunakan metode deskriptif kualitatif [19], yang artinya hasil penelitian ini di deskripsikan dalam bentuk penjelasan dan uraian kalimat-kalimat yang mudah dimengerti, menginterpretasikan atau melakukan

[18] Abdulkadir Muhammad, *Op.Cit.*, hlm. 192.

[19] *Ibid.*, hlm. 152.

penafsiran terhadap data yang telah dikumpulkan untuk dapat ditarik kesimpulan mengenai Kebijakan Formulasi terhadap Kejahatan Siber berdasarkan Asas Legalitas.

HASIL PENELITIAN

Menyikapi maraknya kasus tindak pidana cybercrime ini, maka dilakukan berbagai upaya penanggulangan tindak pidana sebagai berikut :

1. Sarana Penal (Kebijakan Penal)

Kebijakan Penal (kebijakan dalam hukum pidana) adalah salah satu kebijakan dalam penanggulangan kejahatan dengan menggunakan hukum pidana. Kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materiil, hukum formil dan penitentier dalam masyarakat. Dalam Kongres PBB ke-4 yang berlangsung di Kyoto, disepakati bahwa usaha pencegahan kejahatan termasuk penerapan hukum pidana merupakan bagian integral dari rencana pembangunan nasional[20]. Kebijakan hukum pidana pada hakikatnya merupakan usaha untuk mewujudkan peraturan perundang-undangan pidana agar sesuai dengan keadaan pada waktu tertentu (*ius constitutum*) dan masa yang akan datang (ius constituendum)[21]. Dalam upaya menanggulangi tindak pidana cybercrime, resolusi Kongres PBB VIII/1990 mengenai computer related crimes mengajukan beberapa kebijakan antara lain:

[20] Widodo, op.cit, hlm. 188

[21] Lilik Mulyadi, Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik, Bandung: PT. Alumni, 2008, hlm. 390.

a. Menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer, lebih efektif dengan mempertimbangkan langkah-langkah berikut :

1) Melakukan modernisasi hukum pidana meateriil dan hukum acara pidana.
2) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer.
3) Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer.
4) Melakukan upaya-upaya pelatihan bagi para hakim, penegak hukum, dan pejabat, mengenai kejahatan dibidang ekonomi dan cybercrime.
5) Memperluas rules of ethics dalam penggunaan computer, dan mengajarkannya melalui kurikulum informatika.
6) Mengadopsi kebijakan perlindungan korban sesuai deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban

melaporkan adanya kejahatan siber.

b. Menghimbau agar negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan tindak pidana cybercrime.

c. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan PBB untuk:

1) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi cybercrime di tingkat nasional, regional, maupun internasional.

2) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan cybercrime dimasa mendatang.

3) Mempertimbangkan cybercrime sewaktu meninjau pengimplementasian perjanjian ekstradisi, dan bantuan kerjasama dibidang penangulangan kejahatan[22]

2. Sarana Non Penal (Kebijakan Non Penal)

Kebijakan non penal dapat ditempuh dengan cara memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang, baik secara formal maupun non

[22] Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Jakarta: PT RajaGrafindo Persada, hlm. 3.

formal, terutama kepada pihak yang rentan melakukan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan tindak pidana cybercrime, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum perdata, yang berhubungan dengan penyelenggaraan sistem dan jaringan komputer. Hal ini senada dengan Convention on *Cyber Crime*, bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan kejahatan siber adalah perjanjian ekstradisi, mutual assistence in criminal matters, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk mengumpulkan alat bukti elektronik. Bantuan-bantuan tersebut berupa fasilitas atau bantuan lain, dengan syarat dan izin oleh hukum nasional masing-masing Negara. Dalam hal ini diatur pula pertanggungjawaban korporasi, baik dalam hukum pidana, maupun dalam hukum perdata dan hukum administrasi.

KESIMPULAN

Bahawa masih banyak kejahatan siber yang perlu dirumuskan dalam perundang-undangan Hukum Pidana berikutnya

Berbagai upaya penanggulangan tindak pidana cybercrime dilakukan, meliputi atas:

a) Sarana Penal (Kebijakan Penal) adalah salah satu kebijakan dalam penanggulangan kejahatan dengan

menggunakan hukum pidana. Kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materiil, hukum formil dan penitentier dalam masyarakat.

b) Sarana Non Penal (Kebijakan Non Penal)

Kebijakan non penal dapat ditempuh dengan cara memperbaiki perekonomian nasional, melakukan pendidikan budi pekerti kepada setiap orang, baik secara formal maupun non formal, terutama kepada pihak yang rentan melakukan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengefektifkan kerjasama internasional dalam pemberantasan tindak pidana cybercrime, memperbaiki sistem pengamanan komputer, serta mengefektifkan hukum administrasi dan hukum perdata, yang berhubungan dengan penyelenggaraan sistem dan jaringan komputer.

Sarana dan kebijakan yang ada diharapkan dapat menanggulangi tindak pidana cybercrime, walaupun tidak bisa sepenuhnya bisa mengatasi tindak pidana tersebut. Peningkatan kualitas sarana dan kebijakan dalam menanggulangi kejahatan ini yang sangat dibutuhkan

DAFTAR PUSTAKA

Buku-Buku

Abdulkadir Muhammad, *Hukum dan Penelitian Hukum,* PT Citra Aditya Bakti, Bandung, 2004.

A.Hamid S. Attamini, *Teori Perundang-undangan Indonesia*, makalah pada Pidato Upacarapengukuhan Guru Besar tetap di Fakultas Hukum UI, Jakarta, 1992.

Arief Mansyur, Dikdik M. dan Gultom, Elisatris, *Urgensi perlindungan korban kejahatan: antaranorma dan realita*, RajaGrafindo Persada, Jakarta, 2007.

Barda Nawawi Arief, Tindak Pidana Mayantara, *Perkembangan Kajian Cybercrime di Indonesia*,RajaGrafindo Persada, Jakarta, 2006.

----------*RUU KUHP Baru Sebuah Resrukturisasi/Rekonstruksi Sistem Hukum Pidana Indonesia*,Semarang: Badan Penerbit Universitas Diponegoro, 2009.

----------B*unga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHPBaru*, Bandung: Citra Aditya Bakti, 2014.

----------*Antisipasi Penanggulangan* "*Cybercrime*" *dengan hukum Pidana*, PT RajaGrafindo,Jakarta.

----------*Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam PenanggulanganKejahatan*, Kencana Prenada Media Group, Jakarta (Selanjutnya disebut Barda Nawawi Arief II), 2010.

Budi Sutedjo Dharma Oetomo, *E-education : Konsep, Teknologi dan Aplikasi Internet Pendidikan*,Andi, Yogyakarta, 2007.

Eddy O.s Hiariej, *Asas Legalitas dan Penemuan Hukum dalam Hukum Pidana,* Erlangga, Jakarta,2009.

Horton, Paul B dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984.

Fahmi Anwar, *Perubahan dan Permasalahan Media Sosial* , Jurnal Muara Ilmu Sosial, Humaniora, danSeni Vol. 1, No. 1, April 2017.

Jazim Hamidi dan Mustafa Lutfi, *Hukum Lembaga Kepresidenana Indonesia*, Alumni, Malang, 2009.

Kelik Pramudya, dkk, 2010, *Pedoman Etika Profesi Aparat Hukum*, Yogyakarta, Pustaka Yistisia.

L. J. Van Apeldoorn, "Pengantar Ilmu Hukum", cetakan kedua puluh enam Pradnya Paramita,Jakarta, 1996.

Moh. Kusnardi, *Hukum Tata Negara Indonesia*, Sinar Bakti, Jakarta, 1987.

Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi, *Cyber*Policy Club dan

Indonesia Media Law and Policy Center, 2003.

Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, PT. Bina Ilmu, Surabaya, 1987.

Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000.

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

Soerjono Soekanto, *Penelitian Hukum Normatif Suatu Pengantar*, Rajawali Press, Jakarta, 2006.

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, *Cybercrime-Motif dan Penindakan*, Pensil 324,Jakarta.

Peraturan Perundang-Undangan

Undang-Undang Dasar 1945

United Nations Commision on International Trade Law (UNCITRAL) Mode Law on Electronic Commerce with Guide to Enactment 1996

Kitab Undang-Undang Hukum Pidana

Law of Malaysia At 758 Electronic Commerce Act 2006

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Sumber Lain-Lain

Gustav Radbruch dalam Dwika,"*Keadilan dari Dimensi Sistem Hukum*", http://hukum.kompasiana.com, (02/04/2011), diakses pada 3 April 2021

Pan Mohamad Faiz, 2009. "Teori Keadilan John Rawls", dalam Jurnal Konstitusi, Volume 6 Nomor 1.

Raja Nur Afiqah Zulkifli, dkk., *Satira Politik: Analisis Internet Trolling di Malaysia* , Jurnal Komunikasi Malaysian Journal of Communication , Jilid 34(2) 2018: 223-242.

Vivi Ariyanti, Pembaharuan Hukum Pidana di Indonesia yang Berkeadilan Gender dalam Ranah Kebijakan Formulasi, Aplikasi, dan Eksekusi, Volume 3 Issue 2, September 2019, HOLREV. Faculty of Law, Halu Oleo University, Kendari, Southeast Sulawesi.