BAB II

BENTUK DAN AKIBAT PERUNDUNGAN SIBER DI INDONESIA

1. Perundungan Siber

Secara etimologi *bully* yang dalam bahasa Indonesia sering digunakan dengan bahasa "rundung" yang artinya mengganggu, mengusik terus menerus, menyusahkan.[1] Penelitian menunjukkan pada mulanya perundungan dilakukan secara fisik, dan modelnya juga semakin meluas pada verbal atau psikologis, dan hal tersebut terjadi secara *offline* dan virtual (*online*).[2]

Tindakan negatif yang sering dianggap sepele oleh sebagian besar warga Indonesi adalah perundungan siber, apalagi kalau tindakan tersebut dilakukan oleh anak-anak yang dianggap wajar ketika melakukan tindakan perundungan.

Beberapa penelitian menunjukkan kalau pada mulanya perundungan terjadi hanya pada fisik, namun seiring dengan berkembangya teknologi perundungan terjadi dan melebar tidak hanya pada aspek fisik akan tetapi bentuk perundungan itu semakin melebar yang juga merambah pada verbal dan atau psikologi yang pelaksanaannya dilakukan di dunia maya.

Perundungan siber yang paling banyak terjadi melalui media sosial seperti *facebook* dan *twitter*. Salah satu penelitian ini dilakukan oleh *we are social* yang dilakukan pada bulan Januari 2014 menunjukkan bahwa dari

[1] Rulli Nasrullah, 2015, "*Media Sosial (Perspektif Komunikasi, Budaya dan Teknologi)"*, Simbiosa Rekatama Media, Bandung, h. 187

[2] Ibid

kurang lebih 251 juta jiwa penduduk Indonesia, diperoleh data 38 juta pengguna internet, untuk pengguna *facebook* sebanyak 62 juta atau 25% dari total penduduk Indonesia.[3]

Pada bulan Maret 2015, *facebook* menempati peringkat pertama dengan jumlah pengguna terbanyak di dunia. Berikut ini data jumlah pengguna media sosial di dunia :[4]

Tabel 1.1

No	Jenis Media Sosial	Jumlah Pengguna (dalam jutaan)
1	Facebook	1.415
2	QQ	829
3	WhatsApp	700
4	Qzone	629
5	Facebook Mesenger	500
6	WeChat	468
7	Linkedin	347
8	Skype	300
9	Google+	300
10	Instagram	300
11	Baidu Tieba	300
12	Twitter	288
13	Viber	236
14	Tumblr	230
15	Snapchat	200
16	Line	181
17	Sina Weibo	167
18	Vkontakte	100

Dari data tersebut, maka kemungkinan untuk perbuatan perundungan siber akan semakin meningkat seiring dengan semakin banyaknya pengguna media sosial yang dalam hal ini adalah *facebook* dengan

[3] Rulli Nasrullah, 2015, *Media sosial (Perspektif Komunikasi, Budaya, dan Sosioteknlogi)* Simbiosa Rekatama Media, Bandung, h. 12

[4] Ibid, h. 98

pengguna terbesar di dunia. Tidak lepas pula warga Indonesia yang secara intens meggunakan media sosial tersebut.

Pada tanggal 28 Pebruari 2016, *twitter* Indonesia ramai dengan tagar atau *hastag* #RIPUus. Tagar tersebut merupakan akromin dari *rest in peace* atau beristirahat dengan tenang yang merupakan ungkapan yang biasanya digunakan manakala ada orang yang meninggal dunia, tagar tersebut sempat menjadi trending topik utama di *twitter* Indonsia selama kurang lebih 6 jam.

Topik tren ini bermula ketika salah seorang komika terkenal dari acara *stand up* komedi yang bernama Rizky Firadus Wijaksana atau lebih dikenal dengan panggilan Uus yang mengunggah tulisan di akun twitternya pada tanggal 27 Pebruari 2016 akun twitter @Uus_ "kok ga ngasih tau mereka, bang G-Drgon jangan narkoba dong, bang Siwon jangan homo dong, nggak kan ?" setelah mengunggah tulisan tersebut Uus kembali mengunggah tulisan di akun twitternya, "mending liat cewek pake baju sexy di tempat dugem sambil mabok2 daripada liat cewek hijab di konser korea sambil nangis2 Pfft."

Unggahan tersebut mempunyai maksud mengkritik fans k-pop yang beranggapan Uus sudah menghina idola mereka, akhirnya berakibat Uus mendapat berbagai macam pesan komentar di akun twitternya yang berisi hinaan, caciaan, makian, sampai dukungan terhadap Uus. Agar komentar para fans dengan konten postingan Uus dapat terhubung, mereka menggunakan tagar #RIPUus yang sehingga menjadi trending topik di twitter Indonesia. Dan

ternyata cacian, hinaan, dan makian tersebut tidak hanya ditujukan kepada Uus saja akan tetapi hal itu juga ditujukan untuk teman wanita Uus yang bernama Kartika, fans k-pop menulis "Kartika lebih pantas disebut hina karena penampilannya yang seksi."[5]

Dari kasus tersebut diatas, jelas bahwa perilaku atau perbuatan yang dilakukan oleh fans k-pop kepada Uus dapat dikategorikan dalam perundungan siber yang menurut Hertz bahwa perundungan siber adalah merupakan bentuk penindasan atau kekerasan dengan cara mengejek, mengatakan kebohongan, melontarkan kata-kata kasar, menyebarkan rumor maupun melakukan ancaman atau berkomentar agresif yang dilakukan melalui media-media seperti e-Mail, *chat room,* SMS, *website*, dan lain sebagainya. Dan pada kasus yang menimpa Uus tersebut menggunakan media sosial utama yaitu *twitter*.

Pada waktu awal muncul kejahatan siber diartikan sebagai kejahatan komputer (*computer crime*), *the British Law Commission* mengartikan *Computer Crime* adalah memanipulasi komputer menggunakan berbagai cara yang bisa dipakai dengan itikad buruk agar dapat memperoleh barang, uang atau keuntungan lainnya atau yang dimaksud untuk menimbulkan kerugian pada pihak lain.

Mandell membagi *computer crime* menjadi dua kegiatan, yaitu ;

a. Komputer yang digunakan untuk melaksanakan perbuatan pencurian, penipuan, atau semua perbuatan dengan tujuan mendapatkan keutungan,

[5] *"RIPUus Gaunya otak lu sumpah, jelas-jelas calon bini lu lebih Hina daripada cewek hijabers nonton konser sambil nangis!"* (akun twitter @elisa_ekka, 5 Maret 2016)

keuntungan dalam bisnis, memperoleh kekayaan atau untuk mempeoleh pelayanan;

b. Ancaman terhadap perangkat komputer, seperti tindak pencurian *hardware* atau perangkat lunak, sabotase dan pemerasan.[6]

Pada awal mulanya para ahli hukum terfokus pada *device* (perangkat) yaitu komputer, namun setelah adanya perkembangan teknologi informasi yang bernama internet maka fokus dari identifikasi terhadap definisi cyber crime lebih diperluas yaitu seluas aktivitas yang dilakukan di dunia cyber dengan menggunakan sistem informasi. Jadi tidak hanya pada komponen hardware saja kejahatan itu diartikan *cyber crime*, akan tetapi sudah diperluas lagi pada wilayah yang disinggahi oleh sistem TIK bersangkutan. Jadi lebih tepat apabila pendefinisian dari *cyber crime* yaitu kejahatan teknologi informasi, juga sebagai kejahatan dunia maya.

Tindak kejahatan pada bidang teknologi informasi ini bisa dikategorikan sebagai *white colour crime* sebab pelaku kejahatan ini merupakan orang yang menguasai internet serta aplikasinya atau orang yang ahli dibidangnya.

Teknologi sampai sekarang mengalami perkembangan amat pesat, hal ini di dukung pula dengan kondisi yang tidak memungkinkan kita melaksanakan kegiatan secara langsung. Mulai dari sekolah, jual beli, dan lain sebagainya semua dilakukan secara online dengan memanfaatkan teknologi.

---

[6] Sahariyanto, Budi, 2012, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Press, Jakarta, h. 10

Begitu juga dalam pelaksanaan praktik hukum di Indonesia, dalam pelaksanaan litigasi juga sudah menerapkan e-litigasi di beberapa pengadilan di Indonesia. Untuk praktik notaris juga sekarang sudah menggunakan *cyber notary* yang pada praktiknya semua urusan dilaksanakan dengan menggunakan teknologi.

Dengan semakin terbukanya teknologi atau TIK tidak menutup kemungkinan untuk para penjahat melakukan tindak kejahatan dengan lebih canggih, yang oleh karenanya muncul kejahatan siber yang dilakukan dengan berbagi metode dan cara. Ada yang melakukan hacking, cracking, pishing, carding, dan beraneka macam lainnya, semua menggunakan teknologi yang sekarang berperan penting dalam kegiatan sehari-hari.

Hak dan kebebasan menggunakan serta memanfaatkan teknologi informasi dilakukan dengan mempertimbangkan pembatasan yang ditetapkan dengan undang-undang yang bermaksud untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai, agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.[7]

Keadilan di Indonesia tergambar dalam Pancasila yang termaktub pada sila ke lima, keadilan sosial bagi seluruh rakyat Indonesia. Sila tersebut mengandung nilai-nilai yang merupakan tujuan dalam kehidupan bermasyarakat, keadilan tersebut didasari serta dijiwai dengan hakekat keadilan kemanusiaan. Maksud yang terkandung adalah keadilan yang dalam

[7] Danrivanto Budhijanto, 2019, *Cyber Law Dan Revolusi Industri 4.0*, Logoz Publishing, Bandung, h. 13

hubungannya antara manusia dengan dirinya sendiri, manusia dengan manusia lainnya, manusia dengan masyarakat, bangsa, dan negara, serta hubungan antara manusia dengan Tuhannya.[8]

Menurut Mas Wigrantoro Roes Setiyadi bahwa, kejahatan siber dikelompokkan menjadi dua, yaitu:

1. Kejahatan biasa yang dalam pelaksanaannya menggunakan media teknologi sebagai alatnya. Pada perbuatan pidana ini, terjadi modus operandi yang meningkat pada yang awalnya memakai peralatan yang biasa / manual, dan saat ini sudah memakai TIK. Adapun efek dari perbuatan kejahatan yang sudah memakai teknologi informasi ternyata sangat serius, utamanya kalau dilihat dari wilayah serta kerugian yang ditimbulkan dari kejahatan itu. Pembobolan rekening, penipuan, pencemaran nama baik, pornografi, perjudian, terorisme, sampai dengan beanja barang dengan memakai kartu kredit hasil mencuri dengan melalui media internet bisa menelan korban di wilayah hukum negara lain, suatu hal yang sangat jarang sekali terjadi pada kejahatan konvensional.
2. Kejahatan yang muncul pasca munculnya internet, yang mana korbannya adalah sistem komputer. Jenis kejahatan pada kelompok ini semakin bertambah sejalan dengan semakin majunya teknologi tersebut. contohnya pengerusakan situs-situs internet, penyebaran virus juga program-program komputer yang mempunyai tujuan merusak sistem komputer.[9]

---

[8] M. Agus Santoso, 2014, *Hukum Moral dan Keadilan Sebuah Kajian Filsafat Hukum*, Kencana, Jakarta, h. 86

[9] Mas Wigrantoro Roes Setiyadi, 2003, *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, GIPI-Indonesia, h. 4

Pada umumnya, kejahatan siber dilakukan oleh insider (orang dalam) yang sudah pernah bekerja di institusi tertentu yang punya kelengkapan alat komputer, telekomunikasi dan informasi, karena mereka mengetahui kelemahan sistem pengamanan yang ada pada institusi tersebut baik *hardware* maupun *software*.

Perundungan merupakan perbuatan negatif yang dilakukan kepada orang lain secara kontinyu atau berulang. Perbuatan ini sering kali dilakukan dan menyebabkan korban menjadi tidak berdaya dan terluka baik mental maupun fisik.

Banyak sekali anak dibawah umur menjadi korban di internet, istilah ini kemudian terkenal dengan istilah perundungan siber, yakni perilaku seseorang untuk melecehkan atau merendahkan seseorang baik dilakukan dengan menggunakan media online maupun dengan menggunakan telepon seluler.[10]

Menurut Sutarman ; "kerugian besar dan penyimpangan sudah terjadi dan sudah dirasakan oleh warga di hampir seluruh dunia dan kerugian yang mempunyai dampak luas di sektor-sektor bidang ekonomi, moneter, perbankan dan bidang lain yang memakai komputer jaringan. Untuk mengantisipasi supaya tidak terkucilakn dalam pergaulan global, maka pemerintah Indonesia harus mengantisipasi dan melakukan langkah nyata dalam menanggulangi kejahatan siber. Langkah itu bisa diambil dengan

[10] Donny BU (ICT Watch), 2013, "*Usir Galau dengan Internet",* Andi Offset, Yogyakarta, h. 41

mengusulkan tindakan preventif berupa dilahirkannya peraturan perundang-undangan yang spesifik di bidang kejahatan siber."[11]

Peristiwa-peristiwa kejahatan yang banyak terjadi akhir-akhir ini di Indonesia banyak dilakukan dengan menggunakan peralatan teknologi, mulai dari penipuan, pencemaran nama baik, pembobolan rekening bank, tindak pidana terorisme dan lain sebagainya. Pemanfaatan teknologi juga sudah mengubah tata hidup masyarakat maupun peradaban manusia yang terjadi secara universal. Perkembangan TIK menyebabkan perubahan ekonomi, budaya, dan sosial dengan sangat cepat. Selanjutnya perkembangan internet, juga menjadi sebab munculnya tindak kejahatan yang disebut dengan *cyber crime* atau kejahatan yang dilakukan dengan memanfaatkan media internet.

Munculnya kasus-kasus kejahatan siber di negara kita ini, seperti hacking situs, *carding,* menyadap transmisi data orang, misalnya pesan elektronik (*e-mail*), serta manipulasi data dengan menggunakan cara mempersiapkan instruksi khusus ke dalam program aplikasi komputer.

Permasalahan secara yuridis untuk menjerat pelaku kejahatan siber ini biasanya berkaitan dengan berbagai persoalan yang berhubungan dengan beberapa karakteristik kejahatan siber, yaitu ;[12]

Pertama, siapakah yang berwenang mengatur atau membuat regulasi yang berkaitan dengan kejahatan di Internet mengingat kejahatan ini melintasi batas

---

[11] Sutarman, 2007, *Cyber Crime Modus Operandi dan Penanggulangannya*, Laks Bang Presindo, Yogyakarta, h. 3

[12] Abdul Wahid, 2005, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, h. 28

teritorial atau *borderless territory*, atau bahkan bisa dikatakan di luar teritorial negara (*out of the state territory*) yang pada akhirnya berkaitan dengan yurisdiksi mana yang berhak untuk melakukan proses peradilan.

Kedua, berkaitan dengan asas legalitas yang sangat fundamental dalam hukum pidana, apakah kejahatan dalam dunia maya dapat dijerat dengan hukum pidana melalui cara penafsiran, mengingat kejahatan tersebut merupakan sesuatu yang sama sekali baru. Sementara umumnya hukum pidana hanya menerima penafsiran otentik saja, di samping berbagai persoalan lain yang berkaitan seperti alat bukti elektronik dan sebagainya sebagai kelanjutannya.

Persoalan tersebut sebenarnya berkaitan dengan kebijakan hukum pidana (*penal policy*) yang Marc Ancel mendefinisikan kebijakan hukum pidana tersebut sebagai suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif.

Di sisi yang lain upaya perumusan hukum pidana secara lebih baik, yang didalamnya mencakup kebijakan untuk merubah atau membuat aturan khusus yang berkaitan dengan kejahatan dunia maya. Artinya meskipun secara esensial bisa dianalogikan dengan kejahatan atau tindak pidana yang diatur di dalam KUHP, akan tetapi menurut pendapat ahli bahwa hukum pidana tidak menerima analogi. Moeljanto menyatakan bahwa asas legalitas mengandung pengertian yang diantaranya adalah untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi, dengan demikian maka secara *a contrario* penafsiran ekstensif tidak bertentangan dengan ketentuan pasal 1 KUHP.

Hukum positif yang secara umum berlaku dapat dikenakan juga untuk para pelaku kejahatan siber, utamanya untuk mereka yang melakukan kejahatan yang menggunakan komputer antara lain pasal-pasal dalam KUHP yang bisa dikenakan antara lain ;

a. Pasal 362 KUHP berlaku juga untuk kasus *carding*, dimana pelaku melakukan pencurian nomor dari kartu kredit (*credit* card) milik orang lain meskipun hal itu tidak dilakukan secara fisik.
b. Pasal 378 KUHP juga dapat dikenakan kepada pelaku penipuan yang dilakukan dengan media elektronik, misalnya dalam contoh perbuatan jual beli secara online barang yang dikirim tidak sama dengan yang dipesan.
c. Pasal 311 KUHP bisa diberlakukan untuk pelaku mencemarkan nama baik seseorang dengan memakai media TIK.
d. Pasal 303 KUHP, untuk pelaku judi online dengan penyelenggara dari Indonesia.
e. Pasal 282 KUHP, berlaku untuk pelaku penyebaran pornografi atau website porno.
f. Pasal 406 KUHP untuk pelaku kasus *deface* atau *hack* yang berdampak menjadikan rusak sistem orang lain.

Pemanfaatan media sosial sebagai media komunikasi menjadi sebab tumbuh subur serta berkembangnya perundungan siber, pada umumnya perbuatan perundungan itu dilakukan melalui media sosial seperti, Yahoo Messenger, Facebook, dan lain-lain. Cara membulinya juga bermacam-macam, mulai dari melakukan pengancamanan, penghinaan, penyebaran isu

atau berita yang tidak benar (palsu), bahkan ada juga yang sampai pada tindakan asusila.

Tindakan pelaku juga dilakukan dengan cara mencuri atau menghack password akun milik korban, kemudian pelaku mengupdate status dengan kata-kata atau dengan mengunggah gambar yang tidak senonoh. Perundungan siber sangat mudah dilaksanakan oleh karena pelaku dan korban tidak saling berhadapan. Sisi yang lain, perundungan siber agak sulit di identfikasi oleh para guru dan orang tua karena sekarang hampir semua anak usia sekolah menengah sampai anak Sekolah Dasar sudah mempunyai akun jejaring sosial.

Faktor pendidikan merupakan salah satu faktor penting selain faktor keluarga, dimana sekolah merupakan tempat pendidikan keilmuan bagi anak. Di sekolah anak-anak berinteraksi dengan teman-temannya yang mana karakter setiap anak adalah berbeda, ada yang bisa memberikan pengaruh positif dan ada juga yang memberikan pengaruh negatif yaitu adanya praktek perundungan, mencuri sampai pada perkelahian. Maka peran guru menjadi sangat penting untuk perkembangan karakter anak sebagai siswa.[13]

Kasus perundungan dengan menggunakan sosial media menjadi masalah serius, sukar untuk dikendalikan oleh para guru dan orang tua karena pelaku yang tidak nampak. Dampak perundungan siber lebih serius dari tindakan perundungan tradisional, karena dalam perundungan siber memberi kesempatan banyak orang untuk melakukannya (baik yang dikenal maupun

[13] Dewa Krisna Prasada, "Pengaturan Delik Pidana Terkait Tindakan Bullying Bagi Anak di Bawah Umur", *Acta Comitas Jurnal Hukum Kenotariatan*, No. 2, Vol. 4, Agustus, 2019, h. 169

yang tidak dikenal). Pada beberapa kasus perundungan siber menjadikan korban depresi serta gelisah, bahkan bunuh diri.[14]

Adanya kejahatan siber sudah menjadi ancaman keamanan, hingga pemerintah atau negara sukar untuk mengimbangi teknik para penjahat yang dilakukan dengan menggunakan teknologi komputer khususnya dengan menggunakan media jaringan intranet dan internet. Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, hingga pada setiap perkembangannya pada hakikatnya membawa dampak seperti dua sisi mata uang yang tak bisa dipisahkan.

2. Bentuk Perundungan Siber Di Indonesia

Perkembangan teknologi informasi menjadikan dunia menjadi tidak ada batas dan menjadi penyebab perubahan sosial secara cepat. Dengan perkembangn teknologi informasi yang sedemikian pesat selain menjadi penyebab perubahan cepat dalam peningkatan kesejahteraan, peradaban, dan kemajuan manusia, juga dapat menjadi media atau sarana yang efektif untuk melakukan perbuatan melawan hukum.

Dan saat ini sudah hadir istilah hukum siber, yang dapat dipahami dengan istilah *cyber law* yang dalam dunia internasional dipakai sebagai istilah hukum yang berkaitan dengan pemanfaatan teknologi informasi. Istilah yang digunakan ialah Hukum Teknologi Informasi (*Law of Information*

[14] Lianthy Nathania Paat, "Kajian Hukum Terhadap Cyber Bullying Berdasarkan Undang-Undang Nomor 19 Tahun 2016", *Lex Crimen,* No. 1, Vol. IX, Jan-Mar, 2020, h. 13

Technology), ada juga istilah *virtual world law* (hukum dunia maya) dan hukum mayantara.[15]

Seseorang yang menggunakan media sosial diperbolehkan mengakses media sosial dengan memakai rangkaian internet meskipun dengan akses yang sangat lambat. Pengguna media sosial dapat melakukan editing, menambahkan, serta merubah aneka model content lainnya. Hal ini sekarang menjadi trend khususnya dikalangan anak muda.

Pasal 27 Undang-Undang ITE No 11 Tahun 2008, pada BAB VII tentang Perbuatan Yang Dilarang, menyebutkan :

(1) Orang dengan secara sengaja dan tidak memiliki hak untuk mendistribusikan dan/atau mentransmisi dan/atau membuat Informasi Elektronik bisa di akses dan/atau elektronik dokumen yang mengandung unsur pelanggaran atas norma atau kesusilaan.
(2) Semua orang yang sengaja serta tidak memiliki hak untuk mendistribusikan dan/atau memberikan informasi elektronik dan/atau dokumen elektronik yang mempunyai tujuan melakukan perjudian dan dapat diakses secara umum.
(3) Semua orang yang sengaja serta tanpa hak mengedarkan atau menjadikan informasi elektronik atau dokumen elektronik yang mempunyai unsur menghina dan/atau mencemarkan nama baik serta dapat diakses secara umum.

[15] Ahmad M. Ramli, 2004, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung, h. 1

(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 unsur pemerasan dan/atau pengancaman.[16]

Di wilayah bidang pendidikan, kasus perundungan siber semakin memprihatinkan, karena pengguna internet sebagian besar merupakan anak usia sekolah menengah dan sekolah dasar, tidak sedikit peserta didik menjadi korban dari perundungan siber. Adapun salah satu cara untuk mengatasi terjadinya perundungan siber di kalangan siswa adalah dengan menekankan nilai-nilai keagamaan secara konsisten.

Kejahatan perundungan siber banyak mengambil target remaja dan anak-anak karena pada kedua jenjang usia tersebut sangat dekat dengan teknologi, disamping itu kedua jenjang usia tersebut masih belum bisa membedakan baik dan buruk dalam dunia teknologi.

Anak yang belum cukup umur dan/atau belum berusia 16 tahun dalam idiom KUHP disebut dengan *minderjarig*, apabila berhadapan di peradilan maka hakim dapat memerintahkan pihak yang bersalah untuk dikembalikan kepada orang tua atau walinya dengan tanpa dijatuhi pidana apapun atau anak tersebut diserahkan kepada pemerintah serta kejahatannya belum lewat 2 tahun dari sejak pelaku dinyatakan bersalah. Hal tersebut disebutkan dengan jelas dalam pasal 45 KUHP.[17]

[16] UU ITE No. 11 Tahun 2008
[17] Dewa Krisna Prasada, op.cit, h. 171

Jenis-jenis perundungan siber dalam buku *save our children from school bullying* adalah sebagai berikut ;[18]

1. *Flaming* (terbakar), yaitu mengirimkan pesan teks yang berisi kata-kata atau kalimat yang penuh dengan amarah serta frontal.
2. *Harassment* (gangguan), adalah pesan-pesan melalui e-mail, *short message system*, maupun teks di sosial media yang berisi gangguan dan dilakukan secara terus menerus.
3. *Denigration* (pencemaran nama baik), adalah proses mengumbar atau menyiarkan keburukan seseorang dengan memakai alat TIK dengan tujuan merusak reputasi atau nama baik seseorang.
4. *Impersonation* (meniru), merupakan tindakan atau perbuatan pura-pura sehingga menyerupai orang lain serta mengirim pesan-pesan atau status yang tidak baik.
5. *Outing*, menyebarkan rahasia orang lain, baik berupa foto, video atau apapun yang bersifat privat kepada publik.
6. *Trickery* (tipu daya), adalah perbuatan membujuk orang dengan memakai tekik tipu daya yang bertujuan untuk memperoleh rahasia atau hal-hal privat korban.
7. *Exclusion* (pengeluaran), tindakan mengeluarkan seseorang dari group online dengan cara yang keji atau kejam dan disengaja.

[18] Dewi dan Purwanti, 2014, *Pengaturan Cyber Bullying dalam Undang-Undang Nomor 11 Tahun 2008*, eJournal yang didownload pada tanggal 20 Desember 2020 dari http://ojs.unud.ac.id/index.php/kerthawicara/article/download/9110/6870

8. *Cyberstalking*, adalah mencemarkan nama baik seseorang dan mengganggu secara kontinyu hingga dapat mengakibatkan ketakutan yang luar biasa pada korban.

Perundungan merupakan tindakan negatif yang dilakukan secara terus menerus dan berulang-ulang, korban dari tindakan ini akan menjadi tidak berdaya dan terluka baik fisik maupun mental. Sebagian orang berpendapat bahwa tindakan perundungan merupakan hal yang wajar dilakukan oleh anak-anak, akan tetapi pada kenyataannya perundungan mempunyai dampak negatif yang besar pada korban.

Menurut Coloroso, perundungan melibatkan empat unsur sebagai berikut ;

1. *Imbalance power* (ketidakseimbangan kekuatan), pelaku perundungan bisa saja orang yang lebih besar, lebih kuat, lebih tua, dan lebih mahir secara verbal, status sosialnya lebih tinggi, atau berasal dari ras yang berbeda.
2. *Desire to hurt* (keinginan untuk mencederai), dalam perundungan tidak ada kekeliruan atau kecelakaan dan tidak ada ketidaksengajaan dalam mengucilkan korban. Perundungan juga bisa menyebabkan kepedihan emosional atau luka fisik. Melibatkan tindakan yang dapat melukai serta bisa menimbulkan rasa senang pada pelaku perundungan pada waktu menyaksikan korban menderita karena perbuatannya.
3. Ancaman agresi lebih lanjut, artinya peristiwa perundungan tidak hanya terjadi sekali, tetapi juga repetitif atau dilakukan secara berulang-ulang.

4. Teror, dalam perundungan yang dimaksud adalah kekerasan secara sistematis yang dipakai untuk melakukan intimidasi serta menjaga dominasi. Sementara teror bukan hanya sebuah cara untuk mencapai tujuan perundungan namun juga sebagai tujuan akhir dari perundungan itu sendiri.

Dalam hal peristiwa perundungan, sebenarnya antara pelaku dan korban secara berama-sama mengalami efek negatif secara psikologis, hingga diperlukan pendidikan etika komunikasi yang bagus dalam bersosial media untuk mengatasi perundungan siber yang makin parah terjadi di sekitar kita.

Pendapat lain tentang pengertian dari perundungan siber adalah Teknologi Informasi dan Komunikasi yang dipergunakan untuk membuat sakit orang lain secara sengaja dan terus menerus. Perundungan siber juga bisa maknai sebagai salah satu model intimidasi yang dilakukan oleh pelaku dengan tujuan melecehkan korban melalui media teknologi.

Tujuan dari pelaku perundungan adalah keinginan untuk melihat seseorang atau korban terluka, sehingga melahirkan banyak cara yang dipakai oleh pelaku untuk menyerang korban dengan pesan-pesan kejam serta gambar-gambar yang mengganggu serta disebarkan dengan tujuan mempermalukan korban dihadapan orang-orang yang melihatnya.

Motivasi pelaku dalam perbuatan ini sangat beragam, bisa jadi hanya sekedar iseng atau bercanda, ingin mencari perhatian, dan ada juga yang memang pelaku sengaja melakukannya karena marah, frustasi dan keinginan untuk balas dendam.

Kekerasan perundungan siber di kalangan remaja dikhawatirkan akan muncul perilaku negatif yang bisa berakibat fatal bila tidak segera diselesaikan dengan baik,. Oleh sebab itu, tindakan preventif harus segera dilakukan untuk menanggulangi masalah tersebut. Tindakan preventif bisa dilakukan mulai dari diri sendiri, seperti contoh menambah wawasan tentang penggunaan teknologi informasi, memperbanyak aktivitas yang positif, serta memperkaya kreativitas yang dapat memberikan manfaat.

Kendati demikian, peran serta orang tua dan keluarga juga sangat dibutuhkan. Seperti mendampingi anak-anak pada saat mempergunakan alat komunikasi, juga membiasakan bersikap terbuka antar masing-masing anggota keluarga.

Internalisasi nilai-nilai pendidikan agama juga bisa dilaksanakan dengan memaksimalkan bidang pendidikan agama di lembaga pendidikan/sekolah, pendidikan agama bisa dilaksanakan dalam rangka memberi peluang pada siswa untuk lebih memahami tentang eksistensi Tuhan serta menjadi sumber dari hidup makhluk sedunia.

Undang-Undang Dasar 1945 hasil amandemen memposisikan Indonesia sebagai negara hukum sebagaimana tertulis pada BAB I pasal 1 ayat (3), selain itu dinyatakan dengan tegas bahwa negara Indonesia ini merupakan negara hukum (*rechtstaat*) dan bukan merupakan negara yang berdasarkan pada kekuasaan belaka (*machstaat*). Artinya Indonesia merupakan negara hukum yang demokratis berdasarkan Pancasila dan Undang-Undang Dasar 1945 yang menjunjung tinggi Hak Asasi Manusia serta menjamin kedudukan

dalam hukum serta pemerintahan semua warga negaranya sama juga adanya kewajiban untuk menjunjung tinggi hukum dan pemerintahan serta tidak ada pengecualian.[19]

Hukum sudah menetapkan apa yang harus dilakukan dan/atau yang boleh dilakukan juga apa yang dilarang untuk dilakukan. Sasaran hukum yang akan dituju bukan hanya orang-orang atau manusia yang melakukan perbuatan melawan hukum, akan tetapi juga perbuatan hukum yang mungkin akan terjadi baik secara konvensional maupun menggunakan media-media elektronik yang dalam hal ini merupakan kejahatan siber, dan juga kepada kelengkapan perangkat negara yang akan bertindak menurut hukum. Sistem kerja hukum yang demikian menjadi salah satu bentuk dari penegakan hukum.

Law enforcement atau penegakan hukum pada pengertian yang lebih luas adalah meliputi kegiatan dalam melakukan serta menerapkan hukum juga melaksanakan tindakan hukum atas semua bentuk pelanggaran dan penyimpangan terhadap hukum yang pelakunya merupakan subyek hukum, baik melalui proses dan prosedur peradilan maupun prosedur arbitrase dan juga mekanisme ADR (*alternative desputes or conflicts resolution)*.

Menurut Soerjono Soekanto, penegakan hukum dipengaruhi oleh faktor-faktor berikut ;

a. Faktor hukumnya sendiri, yakni aturan atau peraturan perundangan yang ada dan diberlakukan di Indonesia;

[19] Kelik Pramudya, dkk, 2010, *Pedoman Etika Profesi Aparat Hukum*, Pustaka Yustisia, Yogyakrta, h. 1

b. Faktor penegak hukum, yaitu para pihak yang membuat serta pihak yang menerapkan hukum;
c. Faktor sarana atau fasilitas yang mendukung penegakan hukum;
d. Faktor masyarakat, yaitu warga atau lingkungan yang mana hukum tersebut diberlakukan dan/atau diterapkan;
e. Faktor kebudayaan, yaitu sebagai hasil karya, cipta dan rasa yang berdasarkan pada karsa manusia dalam pergaulan sosial atau hidup.[20]

Dari ke lima faktor tersebut, sering terjadi saling mempengaruhi antara satu dan yang lain. Eksistensi norma hukum yang dirumuskan dalam UU contohnya berfungsi sebagai *law in books* sudah ditentukan prospeknya di tengah masyarakat dalam sisi *laaw in action* atau hukum dalam realitasnya yang didukung dengan mental penegak hukum. Aparat penegak hukum akan menjadi penentu dalam rangka menegakkan norma hukum.

Alat negara bertanggungjawab dalam menggunakan hukum sebagai senjata untuk melawan berbagai bentuk kejahatan yang akan, sedang, atau sudah mengancam bangsa Indonesia. Alat negara dituntut untuk kerja keras oleh karena perkembangan dalam dunia kriminal, terlebih perkembangan kejahatan dengan menggunakan teknologi atau disebut dengan *cyber crime* yang semakin mengkhawatirkan. Dan alat negara inilah yang menjadi subyek utama untuk berperang dan melawan kejahatan di siber.

Dalam kejahatan di siber perbuatan-perbuatan yang melanggar hukum disini termasuk perbuatan pencurian, penipuan, pelanggaran HAKI

[20] Abdul Wahid, dkk, 2005, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, h. 136

seperti contoh penggandaan dan plagiat hasil karya seseorang, juga kejahatan dan pelanggaran lainnya yang jenis perbuatan-perbuatan tersebut dapat memenuhi unsur *cyber crime* termasuk juga dalam hal ini adalah perundungan siber.

3. Dasar Hukum Perundungan Siber

KUHP menjadi kitab pertama sebagai referensi dalam mencari dan menentukan hukuman kepada pelaku tindak pidana di Indonesia, yang mana KUHP tersebut mengatur tentang hukum pidana secara umum yang biasa disebut dengan pidana umum. Adapun beberapa kasus tindak pidana yang tidak dan/atau belum diatur dalam KUHP diatur secara tersendiri dengan peraturan atau Undang-Undang khusus seperti UU ITE[21] yang kemudian disebut dengan pidana khusus.

Pasal 310, pasal 311, dan pasal 315 KUHP dapat dijadikan sebagai rujukan terhadap tindak pidana perundungan siber, dan untuk sementara ini pasal 315 KUHP merupakan pasal yang sangat tepat untuk menjerat pelaku perundungan siber.[22] Dalam pasal 315 KUHP disebutkan bahwa setiap penghinaan dengan sengaja yang tidak bersifat pencemaran atau pencemaran tertulis yang dilakukan terhadap seseorang baik dimuka umum dengan lisan atau tulisan, maupun dimuka orang itu sendiri dengan lisan atau perbuatan, atau dengan surat yang dikirimkan atau diterimakan kepadanya,

[21] Pradittyo, Randy, "Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Tindak Pidana Pendanaan Terorisme", *Jurnal Rechts Vinding : Media Pembinaan Hukum Nasional*, No. 1, Vol. 5, 2016, h. 17

[22] Muhammad Dani Ihkam, "Tindak Pidana Cyber Bullying Dalam Perspektif Hukum Pidana Indonesia", *Jurnal Kertha Wicara,* No. 11, Vol. 9, h. 5

diancam karena penghinaan ringan, dengan pidana penjara paling lama empat bulan dua minggu atau denda paling banyak tiga ratus rupiah.

Unsur-unsur yang terdapat dalam pasal 315 KUHP yang dapat dijadikan rujukan dalam tindak pidana perundungan siber adalah ;[23]

a. Unsur Obyektif

I. Penghinaan yang tidak bersifat pencemaran lisan atau pencemaran tertulis;

Yang dimaksud dengan unsur I di sini adalah adanya perbuatan menghina atau mencela seseorang dengan tanpa adanya maksud untuk mencemarkan nama baiknya, akan tetapi perkataan yang dilontarkan kepada seseorang tersebut dapat membuat orang lain tersinggung dan merasa harga dirinya sebagai manusia direndahkan.

II. Dilakukan terhadap seseorang dimuka umum dengan lisan atau tulisan, maupun dimuka orang itu sendiri dengan lisan atau perbuatan;

Perbuatan tersebut dilakukan baik secara langsung dihadapan orang yang dimaksud maupun dimuka umum dengan perkataan secara langsung, dengan tulisan atau dengan menggunakan media elektronik.

III. Dengan surat yang dikirimkan atau diterimakan kepadanya.

Tidak pidana dimaksud dalam pasal 315 KUHP dilakukan secara tertulis atau berupa surat yang dikirimkan langsung kepada seseorang dengan maksud menghina sehingga surat atau tulisan tersebut dapat dijadikan sebagai bukti dalam perbuatan penghinaan.

[23] Ndruru, Mana Kebenaran, Ismail Ismail, dan Suriani Suriani, "Pengaturan Hukum Tentang Tindak Penghinaan Citra Tubuh (Body Shaming)", *Jurnal Tectum*, No. 2, Vol. 1, 2020, h. 2

b. Unsur Subyektif

Unsur kesengajaan atau dengan sengaja dalam Kitab Undang-Undang Hukum Pidana belum menjelaskan secara langsung terhadap kata sengaja yang dimaksud dalam perbuatan pidana, namun hal tersebut dapat diketahui arti kata sengaja yang diambil dari *Memorie van Toelicthing* (MvT) yang berarti mengetahui atau menghendaki.[24] Maka dapat dipahami dengan jelas disini bahwa unsur dengan sengaja merupakan tindakan yang dengan sadar dan sengaja dilakukan oleh seseorang untuk melakukan perbuatan pidana dimaksud.

Berdasarkan penjelasan diatas, maka perundungan siber sudah memenuhi unsur-unsur dalam pasal 315 KUHP yang berarti perbuatan perundungan siber tersebut dilakukan baik secara langsung maupun tidak langsung, dengan lisan atau tulisan serta menggunakan media elektronik yang dapat diakses oleh orang banyak dengan maksud serta tujuan menghina seseorang.

Adapun dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik secara khusus terdapat pasal-pasal yang mengatur tindak pidana perundungan siber, antara lain :

1. Pasal 27 ayat (1) kesengajaan yang dilakukan dengan tanpa hak menjadikan dapat diaksesnya dokumen elektronik atau informasi elektronik yang memuat sesuatu yang melanggar kesusilaan.

[24] Saroinsong, Raisa L., "Pertanggungjawaban Terhadap Pelaku Tindak Pidana Pencemaran Nama Baik Berdasarkan Pasal 310 KUHP", *Jurnal Lex Privatum*, No. 7, Vol. 5, 2017, h. 5

2. Pasal 27 ayat (3) kesengajaan yang dilakukan dengan tanpa hak menjadikan dapat diaksesnya dokumen elektronik atau informasi elektronik yang memuat unsur penghinaan dan/atau pencemaran nama baik.
3. Pasal 27 ayat (4) kesengajaan yang dilakukan dengan tanpa hak menjadikan dapat diaksesnya dokumen elektronik atau informasi elektronik yang memuat tentang pemerasan dan/atau ancaman.
4. Pasal 28 ayat (2) kesengajaan yang dilakukan dengan tanpa hak menjadikan dapat diaksesnya dokumen elektronik atau informasi elektronik yang memuat sesuatu yang dapat menyebabkan permusuhan dan/atau menimbulkan kebencian baik individu atau kelompok masyarakat tertentu dan/atau berhubungan dengan SARA.
5. Pasal 29 kesengajaan yang dilakukan dengan tanpa hak menjadikan dapat diaksesnya dokumen elektronik atau informasi elektronik yang memuat unsur ancaman, kekerasan atau menakut-nakuti secara pribadi.

4. Subyek Hukum Perundungan Siber

Perundungan siber dalam pandangan sebagian orang hanya dapat dilakukan dengan cara bertatap muka atau dengan kontak fisik secara langsung, akan tetapi dalam hal ini perbuatan perundungan pada faktanya juga dapat dilakukan dengan memanfaatkan teknologi informasi dan komunikasi atau dikenal dengan istilah perundungan siber.

Perundungan siber dapat juga dikatagorikan sebagai kejahatan siber oleh karena ciri-ciri khusus sebagai berikut ;

1. *Non Violence* (tanpa kekerasan);
2. *Minimize of physical contact* (sedikit melibatkan kontak fisik);
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media, dan informatika) global.[25]

Pada dasarnya kejahatan tumbuh serta berkembang dalam masyarakat, tidak ada kejahatan tanpa adanya masyarakat yang mempunyai penjahat sesuai dengan jasanya. Karena masyarakat banyak yang sudah menggunakan media internet sebagai salah satu media komunikasi pada setiap hari maka hadirlah perundungan siber sebagai salah satu bentuk kejahatan yang kerap terjadi di sekitar kita.

Dalam peristiwa terjadinya perundungan siber ada dua individu yang terlibat ;

1. *The bully* (pelaku) yaitu orang yang secara langsung melakukan agresi baik secara fisik, verbal, maupun psikologis kepada orang lain dengan menggunakan media siber. Untuk selanjutnya pelaku di sini adalah sebagai subyek perundungan siber.
2. *The victim* (korban) adalah orang yang menjadi sasaran atau targer dari perundungan siber yang dilakukan oleh pelaku. Dalam hal ini korban adalah sebagai obyek perundungan siber.

Dalam hal perundungan siber ada terdapat perbedaan dengan perundungan konvensional dimana pada perundungan siber subyek

[25] Didik M. Arief Mansur dan Elisatris Gultom, 2009, *Cyberlaw : Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, h. 27

melakukan perbuatannya dengan menggunakan media teknologi tanpa harus bertatap muka dengan obyek. Dari perbedaan tersebut ditemukan dimana pelaku dapat berupa subyek tunggal yang melakukan agresi terhadap korban yang dalam kejahatan siber pelaku bisa dicirikan menjadi dua, yaitu ;

1. Pelaku utama, yaitu seseorang yang memicu atau yang memulai pertama kali perbuatan perundungan terhadap seseorang. Untuk menetapkan sebagai pelaku utama dapat dilihat pada bentuk postingnya yang memicu baik berupa gambar, status atau apapun yang bertujuan mengejek atau menghina, merendahkan, menyebarkan isu, mengancam, maupun menghancurkan relasi.
2. Pelaku pembantu, dimana pelaku pembantu ini ikut berperan dalam mengirimkan pesan yang bermuatan unsur perundungan siber pada tautan, status, maupun gambar yang diberikan oleh pelaku utama yang ditujukan untuk obyek sasaran yakni korban.

   Pelaku pembantu dapat menjadi representasi wujud perundungan siber yang nyata, dimana mayoritas serangan terhadap korban itu dilakukan oleh pelaku pembantu.[26]

Ada perbedaan dengan pelaku yang memiliki pelaku utama dan pelaku pembantu, dalam kasus perundungan siber yang diteliti korban adalah subyek tunggal atau perseorangan. Ranny Rastati dalam jurnal penelitiannya mengemukakan bahwa perundungan siber selain ditujukan kepada individu

[26] Maulidah Nur Muhlishotin, "Cyber bullying Perspektif Hukum Pidana Islam", *Al Jinayah*, No. 2, Vol. 3, 2017, h. 381

ditemukan pula tiga obyek lainnya, yaitu ; terhadap lokasi, keagamaan, dan institusi atau profesi.[27]

Selanjutnya temuan dari penelitian pada tahun 2011 sampai 2012 yang dilakukan oleh Kementerian Komunikasi dan Informatika bersama UNICEF yang melibatkan 400 anak dan remaja pada rentang usia 10 sampai 19 tahun yang berada di 11 provinsi di Indonesia, hasil dari riset tersebut menunjukkan bahwa 13% mengalami perundungan siber dalam bentuk hinaan, ancaman, dan dipermalukan di media sosial. 9% menyatakan pernah mengirimkan pesan berupa penghinaan dan kemarahan melalui media sosial, 14% mengirimkan melalui pesan teks. Di sini dapat disimpulkan bahwa 13 dari 100 responden merupakan pelaku perundungan siber.[28]

5. Bentuk Perundungan Siber Dalam Undang-Undang ITE

Setiap bentuk pelanggaran atau pun kejahatan berkonsekuensi untuk dapat dikenakan sanksi, begitu juga dengan perbuatan perundungan siber yang dilakukan baik oleh pelaku utama maupun pelaku pembantu sama-sama berpotensi untuk dapat dikenakan sanksi sesuai dengan peraturan perundangan di Indonesia.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 mengatur tentang bagaimana aturan hukum bagi pelaku perundungan siber.

---

[27] Ranny Rastati, "Bentuk Perundungan Siber di Media Sosial Dan Pencegahannya Bagi Korban Dan Pelaku", *Jurnal Sosioteknologi*, No. 2, Vol. 15, 2016, h. 180

[28] Ibid, h. 170

Bentuk-bentuk perundungan siber yang diatur dalam BAB VII Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Jo. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 disebutkan dalam pasal-pasal sebagai berikut ;

1. Pasal 27 ayat (1), menyebarkan informasi yang memiliki muatan melanggar susila.
2. Pasal 27 ayat (3), menghina dan/atau mencemarkan nama baik orang lain dengan menggunakan media TIK.
3. Pasal 27 ayat (4), menyebarkan informasi atau berita dengan menggunakan media elektronik yang mengandung muatan pemerasan dan/atau ancaman.
4. Pasal 28 ayat (2), menyebarkan informasi atau berita dengan menggunakan media elektronik yang bertujuan untuk menimbulkan kebencian dan/atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA).
5. Pasal 29, mengirimkan informasi yang berisi ancaman dan/atau menakut-nakuti yang ditujukan pada individu atau pribadi.[29]

Ketentuan yang disebutkan dalam Pasal 27 ayat (1) UU ITE dapat dijadikan acuan apabila seseorang mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar

[29] UU RI Nomor 11 Tahun 2008 Jo. UU RI Nomor 19 Tahun 2016

kesusilaan, dengan unsur kesengajaan dan tanpa hak maka dapat dikatagorikan ke dalam perbuatan pidana.[30]

Pasal 27 ayat (1) UU ITE ini sangat berkaitan erat dengan hak pribadi seseorang (*privacy rtights*) maka untuk pelaku yang melanggar Pasal 27 ayat (1) UU ITE ini dapat dikenakan sanksi pidana. Adapun unsur-unsur pidana yang terdapat dalam Pasal 27 ayat (1) UU ITE adalah sebagai berikut ;

1. Setiap orang
2. Dengan sengaja dan tanpa hak
3. Mendistribusikan atau mentransmisikan atau membuat dapat diakses
4. Muatan yang melanggar kesusilaan

Subyek delik yang diakui oleh Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tidak hanya perorangan akan tetapi juga korporasi, di sini ada 19 (sembilan belas) perbuatan yang diatur dalam Pasal 27 sampai Pasal 37 jo. Pasal 45 sampai Pasal 51 sebagai berikut ;

1. Setiap orang yang 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;

[30] Lianty Nathania Paat, "Kajian Hukum Terhadap Cyber Bullying Berdasarkan Undang Undang Nomor 19 Tahun 2016", *Lex Crimen,* No. 1, Vol. IX, 2020, h. 18

2. Setiap orang yang 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 yang 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;
4. Setiap orang yang 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;
5. Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohon dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik;
6. 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 antar golongan (SARA);
7. 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;

8. Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun;
9. Setiap orang yang dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik ;
10. Setiap orang yang dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan;
11. Setiap orang yang 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;
12. Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau transmisi informasi elektronik dan/atau dokumen elektronik yang bersifat publik, dari, ke, dan 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 ditransmisikan;

13. Setiap orang yang 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;
14. Setiap orang yang 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;
15. Setiap orang yang 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;
16. Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
    a. Perangkat keras (*hardware*) atau perangkat lunak (*software*) komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai Pasal 33;
    b. Sandi lewat komputer, kode akses, atau hal sejenis dengan itu ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

17. Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang autentik.[31]

Ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) tentang perundungan siber tidak ada, di dalam Kitab Undang-Undang Hukum Pidana (KUHP) hanya ada pasal yang mengatur mengenai pengancaman dan penghinaan saja. Dan dengan adanya Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini merupakan pengaturan khusus dari Kitab Undang-Undang Hukum Pidana (KUHP) sebagaimana asas hukum *lex spesialis derogate legi lex generalis*.

[31] Hanafi Amrani dan Mahrus Ali, 2015, *Sistem Pertanggungjawaban Pidana; Perkembangan dan Penerapan*, Raja Grafindo, Jakarta, h. 96