

BAB III

**UPAYA PEMERINTAH DALAM MENCEGAH
DAN MENANGGULANGI PERUNDUNGAN SIBER DIKAITKAN
DENGAN KONSEP KEADILAN**

1. Hukum Siber Di Indonesia

Hukum pidana adalah salah satu hukum formil yang ada di Indonesia, secara spesifik hukum pidana merupakan seperangkat aturan yang dipergunakan untuk mengatur tentang tindak kejahatan dan pelanggaran. Dalam hal ini diatur secara umum dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang didalamnya memuat buku satu tentang ketentuan umum, buku dua mengatur tentang kejahatan, dan buku tiga tentang pelanggaran. Kejahatan bukan sebuah konsep baru dalam sejarah peradaban manusia, konflik interest antara manusia dan iblis dapat dipandang sebagai embrio kejahatan yang berawal dari perasaan iri, sombong, dan dengki suatu kejahatan itu dimulai.

Induk dari *cyber crime* adalah *cyber space*,¹ ini merupakan sebuah realitas baru yang dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua dengan menggunakan basis protokol. *Transmission Control Protocol (TCP)* atau *Internet Protocol (IP)*. Sistem kerjanya bisa dikatakan bahwa *cyber space* atau internet sudah merubah waktu dan jarak sehingga tidak terbatas.

¹ Maskun, 2012, *Kejahatan Siber (Cyber Crime)*, Kencana Prenada Media Group, Jakarta, h. 46

Menurut Nazura Abdul Manap, *cyber crime* dibedakan menjadi tiga kelompok ;²

1. *Cyber against property*, yang dapat dikategorikan kelompok ini antara lain ; pencurian informasi, properti, dan pelayanan.
2. *Cyber crime against persons*, yaitu meliputi pornografi, *cyber talking*, dan *cyber trespass*.
3. *Spam e-mail, web hacking, breaking, dan cyber terrorism*

Barda Nawawi merumuskan delik-delik yang dikategorikan sebagai kejahatan mayantara dengan merujuk pada *Draft Convention on Cyber Crime* dari Dewan Eropa (*Council of Europe*) No. 25 Tahun 2000 yang berisi delik-delik sebagai berikut :

1. Delik atas integritas, kerahasiaan, dan ketersediaan data dan sistem komputer yaitu :
 - a. Mengakses sistem komputer tanpa hak (*illegal access*).
 - b. Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*).
 - c. Tanpa hak merusak data (*data interface*).
 - d. Tanpa hak mengganggu sistem (*system interface*).
 - e. Menyalahgunakan perelengkapan (*mesuse of device*).
2. Delik-delik yang berhubungan dengan komputer ; pemalsuan dan penipuan (*computer related offences; forgery and fraud*).

² Abdul Wahid, loc.cit, h. 73

3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child phornography*)
4. Delik-delik yang berhubungan dengan hak cipta (*offences-related of infringements of copyright*).

Mardjono Reksodiputro menyimpulkan, bahwa rumusan Barda yang merujuk pada *Draft Convention on Cyber Crime* tersebut bertolak dari definisi *cyber crime* sebagai *crime related technology, computer, and the internet*.

Terminologi *cyber crime* bukanlah merupakan satu-satunya terminologi yang dipakai untuk menggambarkan kejahatan yang sering muncul sejalan dengan terus berkembangnya teknologi informasi dan komunikasi. Adapun terminologi lainnya yang bisa digunakan untuk kejahatan yang berkaitan dengan komputer atau teknologi informasi dan komunikasi antara lain ;

1. *Computer crime*
2. *Computer abuse*
3. *Computer misuse*
4. *Crime by computer*
5. *Computer related crime*
6. *Computer assisted crime*
7. *Internet crime*
8. *e-Crime*

9. *High tech crime*³

Sementara Indra Safitri menjelaskan bahwa *cyber crime* atau kejahatan dunia maya adalah kejahatan yang berhubungan dengan pemanfaatan teknologi informasi dan komunikasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi serta kredibilitas sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.⁴

Dengan semakin berkembangnya teknologi informasi dan komunikasi (TIK), seiring itu pula dalam hukum pidana harus ada pembaharuan, artinya bahwa perbuatan pidana yang dilakukan dengan menggunakan media teknologi tentunya belum atau tidak diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) maka harus ada aturan tersendiri yang mengatur tentang perbuatan atau tindak pidana yang menggunakan teknologi tersebut.

Di Indonesia ada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau dikenal dengan UU ITE, yang secara khusus mengatur segala kegiatan siber yang dilakukan di Indonesia. Tidak lepas juga dari hal tersebut, adanya tindak pidana siber atau yang dikenal dengan *cyber crime* (kejahatan dunia maya), yang mana pelaku kejahatan melakukan aksinya dengan memanfaatkan teknologi informasi dan komunikasi (TIK) atau dengan menggunakan komputer ini juga perlu untuk diatur secara hukum formil di Indonesia.

³ Sigit Suseno, 2012, *Yurisdiksi Tindak Pidana Siber*?, Refika Aditama, Bandung, h. 89

⁴ Abdul Wahid, Loc. Cit, h. 40

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. Pada umumnya, cyber crime 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.

Dengan semakin terbukanya teknologi atau TIK tidak menutup kemungkinan untuk para penjahat melakukan tindak kejahatan dengan lebih canggih, yang oleh karenanya muncul *cyber crime* yang dilakukan dengan berbagai 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.

Sigid Suseno mengatakan dalam bukunya bahwa kejahatan yang timbul dari penggunaan media internet dapat berupa kejahatan jenis baru dan bisa juga berupa kejahatan yang sudah ada sejak lama akan tetapi bentuknya semakin meluas. Semua tindak pidana yang dilakukan di *cyber space* adalah merupakan tindak pidana siber atau disebut juga dengan *cyber crime*.⁵

Perundungan siber yang merupakan salah satu dari bentuk *cyber crime* hingga saat ini masih sering terjadi dan sangat perlu diwaspadai, karena tindakan ini banyak terjadi dikalangan anak-anak dan remaja. Menurut

⁵ Sigid Suseno, 2012, *Yurisdiksi Tindak Pidana Siber*, Rafika Aditama, Bandung, h. 2

Mason, *perundungan siber is an individual or a group willfully using information and communication involving electronic technologies to facilitate deliberate and repeated harassment or threat to another individual or group by sending or posting cruel text and/or graphics using technological means.*⁶

Perundungan merupakan bentuk kekerasan dan intimidasi yang dilakukan oleh seseorang maupun kelompok secara terus menerus yang bertujuan untuk menindas korban, membuat korban menjadi terluka, serta membuat korban kehilangan kepercayaan diri atau pembunuhan karakter.

Perundungan mempunyai tiga unsur yang paling dasar, yaitu ;⁷ perilaku yang mempunyai sifat menyerang (agresif dan negatif), dilakukan secara berulang-ulang, dan terdapat ketidakseimbangan kekuatan diantara pihak-pihak yang terlibat.

Dalam hal perundungan terdapat perbedaan yang jelas antara perundungan tradisional dan perundungan siber, kalau perundungan tradisional dilakukan secara langsung dan berhadapan antara pelaku dan korban sedangkan perundungan siber dilakukan dengan menggunakan media internet atau dilakukan di dunia maya yang artinya antara korban dan pelaku tidak saling berhadapan secara langsung.

Dampak dari terjadinya perundungan siber ini tidak bisa di anggap remeh, karena meskipun perbuatan tersebut tidak dilakukan secara

⁶ Mason, K.L., 2008, *Cyberbullying : A preliminary assesment for school personel*, Psychology in the schools, p. 323

⁷ Dan Olweus, *Bullying at school: What We Know and What We Can Do*. Oxford, Blackwell. 1993, page 9, diakses dari (<http://books.google.co.id/books?id=0Fz1jD9paoQC&printsec=frontcover#v=onepage&q&f=false>), pada tanggal 20 Januari 2021

langsung terhadap fisik korban akan tetapi berdampak pada gangguan psikis, psikologis, dan mental.

Instrumen hukum diharapkan dapat menjadi pelindung bagi korban perlakuan perundungan siber ini masih terdapat ketidakjelasan, artinya masih kabur serta banyak menimbulkan multi tafsir, sehingga bukan tidak mungkin dengan semakin berkembangnya teknologi akan mengakibatkan perundungan siber ini akan semakin meluas dan menjadi kebiasaan yang oleh karena tidak adanya kepastian hukum yang dapat menjadi pelindung dari korban perundungan siber.

Di dalam Kitab Undang-Undang Hukum Pidana (KUHP) ada beberapa pasal yang berhubungan dengan perundungan, Kitab Undang-Undang Hukum Pidana (KUHP) menggunakan salah satunya adalah istilah penganiayaan bukan intimidasi. Disebutkan pada pasal 351 KUHP yang menyebutkan bahwa penganiayaan merupakan perbuatan yang dilakukan dengan sengaja dan ditujukan kepada orang lain sehingga mengakibatkan sakit atau luka.⁸

Pasal 351 KUHP tersebut bisa difahami dengan terjadinya perbuatan penganiayaan itu dilakukan oleh pelaku kepada korban secara langsung, dalam arti terjadi kontak fisik yang sehingga korban menderita luka fisik.

Pasal lain dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang berkaitan erat dengan perundungan atau yang mengenai kekerasan

⁸ Sudarto, 2009, *Hukum Pidana I*, Yayasan Sudarto Fakultas Hukum Undip, Semarang, h. 89

adalah pasal 170, pasal 336, dan pasal 368 KUHP. Biasanya dalam Kitab Undang-Undang Hukum Pidana (KUHP) kekerasan sering dihubungkan dengan ancaman.⁹

Perluasan dari pemahaman tentang kekerasan yang dilakukan dapat dilihat juga dalam pasal 5 Undang-Undang Nomor 23 Tahun 2004 tentang Penghapusan Kekerasan Dalam Rumah Tangga yang menyebutkan bahwa kekerasan dapat dilakukan dengan cara kekerasan fisik, kekerasan psikis, kekerasan seksual, dan penelantaran rumah tangga.

Perundungan siber merupakan kejahatan yang menjadi bentuk perluasan dari perundungan yang dilakukan secara konvensional,¹⁰ perundungan dapat terjadi di lingkungan yang terdapat interaksi sosial seperti;

- a. Sekolah, disebut dengan *school bullying*
- b. Tempat kerja, yang disebut dengan *workplace bullying*
- c. Internet atau teknologi, yang disebut dengan *perundungan siber*
- d. Lingkungan politik, disebut dengan *political bullying*
- e. Lingkungan militer, dikenal dengan *military bullying*
- f. Dalam perpeloncoan, yang dikenal dengan *hazing*

Pemerintah Indonesia dalam hal hukum siber sudah mengeluarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, namun seiring dengan perkembangan teknologi Undang-Undang hadir Undang-Undang Nomor 19 Tahun 2016 Tentang

⁹ Guse Prayudi, *Berbagai Aspek Tindak Pidana Kekerasan Dalam Rumah Tangga*, h. 58

¹⁰ Putri, Marizki. 2018, *hubungan kepercayaan diri dan dukungan teman sebaya dengan jenis perilaku bullying di mtsn lawang mandahiling kecamatan salimpaung tahun 2017*" Menara Ilmu 12, no. 8

Perubahan Atas Undang-Undang Nomor 11 Tahun 2008. Ini menunjukkan bahwa pemerintah Indonesia tidak tinggal diam atas munculnya kasus-kasus siber yang ada dan terjadi di Indonesia.

Dalam rangka mencegah terjadinya tindak pidana siber, maka Undang-Undang ITE tersebut dapat dijadikan dasar hukum dalam proses penegakan hukum atas kejahatan-kejahatan yang dilakukan dengan menggunakan media TIK.

Aspek-aspek penting terkait hukum pidana yang perlu diatur secara jelas antara lain ;

- a. Tanggungjawab penyelenggara sistem elektronik yang perlu adanya pembatasan atau limitasi sehingga tanggungjawab penyelenggara tidak melewati batas kewajaran.
- b. Informasi maupun tanda tangan elektronik yang dihasilkan dari sistem informasi dan print out harus bisa dijadikan sebagai alat bukti di pengadilan.
- c. Perlindungan hukum terhadap bank sentral dan lembaga-lembaga keuangan lainnya dari kemungkinan-kemungkinan gangguan dan ancaman kejahatan siber.
- d. Ancaman pidana yang bersifat *deterren* terhadap tindak kejahatan siber, sehingga bisa memberikan perlindungan terhadap integritas sistem dan

nilai investasi yang telah dibangun dengan alokasi sumber daya yang sangat besar.¹¹

Pada dasarnya perundungan siber mengandung unsur merusak nama baik serta melecehkan seseorang yang hal tersebut bertentangan dengan asas hukum yang berlaku di Indonesia. Demikian pula hal tersebut bertentangan dengan pasal 28G ayat (1) dan (2) UUD RI Tahun 1945 yang berbunyi ;

1. Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.
2. Setiap orang berhak untuk bebas dari penyiksaan atau perlakuan yang merendahkan derajat martabat manusia dan berhak memperoleh suaka politik dari negara lain.¹²

Selanjutnya perundungan siber dalam hukum pidana Indonesia dapat diinterpretasikan dengan berbagai delik yang sudah diatur dalam Kitab Undang-Undang Hukum Pidana, pada Bab XVI tentang penghinaan yang paling relevan dengan tindak pidana perundungan siber adalah pasal 310 ayat (1) dan (2) yang berbunyi sebagai berikut ;

Pasal 310 ayat (1) ;¹³

¹¹ Nazarudin Tianotak, "Urgensi Cyber law di Indonesia Dalam Rangka Penanganan Cyber crime Di Sektor Perbankan, *Jurna Sasi*, No.4, Vol. 17, 2011, h. 25

¹² Pasal 28G UUD NRI Tahun 1945

¹³ Pasal 310 ayat (1) dan (2) Kitab Undang-Undang Hukum Pidana Indonesia

“Barangsiapa dengan sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran, dengan pidana penjara paling lama sembilan bulan atau pidana denda dengan paling banyak empat ribu lima ratus rupiah.”

Pasal 310 ayat (2) ;

“Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.”

Di Indonesia, kebijakan hukum siber atau dikenal dengan *cyber law* termuat dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.¹⁴ Dengan munculnya beberapa kasus terkait dengan hukum siber ini kiranya sangat diperlukan pembaharuan yang lebih spesifik sehingga warga negara Indonesia dapat hidup dengan aman, damai, dan tenang.

Dalam membahas tentang hukum pidana tidak bisa terlepas dari teori pembalasan dan teori relatif yang seakan itu bertolak belakang, akan

¹⁴ Abdul Sakban, Sahrul, Andi Kamawati, “Kebijakan Hukum Pidana Terhadap Kejahatan Cyber Bullying Di Indonesia”, *Jurnal CIVICUS : Pendidikan Pancasila dan Kewarganegaraan*, No. 2, Vol. 7, 2019, h. 60

tetapi pada kenyataan tidak demikian karena pada dasarnya teori gabungan yang memadukan antara teori absolut dengan teori relatif dapat terjadi.¹⁵

Teori gabungan dalam suatu pembenaran pidana terletak pada kejahatan maupun tujuan pidananya, dalam teori gabungan tersebut terdapat tiga golongan yaitu ;

- a. Pidanaan menitik beratkan pada pembalasan yang seimbang dengan perbuatannya dan tidak memiliki standar ketertiban umum;
- b. Pidanaan yang terfokus pada pertahanan, ketertiban umum, dan pidanaan tidak boleh lebih berat dari perbuatan pidana yang dilakukan oleh pelaku;
- c. Fokus pidanaan kepada pembalasan dan pertahanan ketertiban masyarakat dalam posisi yang sejajar.¹⁶

Undang-Undang RI Nomor 8 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Bab XI tentang ketentuan pidana dalam UU ITE dapat diidentifikasi beberapa perbuatan yang dilarang karena memenuhi unsur-unsur pidana yang berkaitan erat dengan perundungan siber sebagai berikut :

1. Pasal 27 ayat (3) mengandung unsur pidana mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Pasal dan ayat ini sesuai dengan bentuk perundungan siber jenis *cyber*

¹⁵ Dewa Krisna Prasada, "Pengaturan Delik Pidana Terkait Tindakan Bullying Bagi Anak Di Bawah Umur", *Akta Comitas Jurnal Hukum Kenotariatan*, No. 2, Vol. 4, 2019, h. 170

¹⁶ Hutahaean B, "Penerapan Sanksi Pidana Bagi Pelaku Tindak Pidana Anak", *Jurnal Yudisial*, No. 6, Vol. 1, 2013, h. 68

- harrasment* (tindakan menyiksa dengan terus menerus menyerang serta mengkritik).
2. Pasal 27 ayat (4) mengandung unsur pidana mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan pemerasan dan/atau ancaman. Pasal dan ayat ini sesuai dengan bentuk perundungan siber jenis *cyber stalking* (perbuatan mengancam, melecehkan, mengganggu seseorang dengan menggunakan media elektronik).
 3. Pasal 28 ayat (2) unsur pidananya adalah adanya penyebaran informasi yang bertujuan untuk menyulut kebencian dan/atau permusuhan antar individu dan/atau kelompok masyarakat tertentu berdasar pada suku, agama, ras (SARA). Pasal dan ayat ini sesuai dengan bentuk perundungan siber jenis *cyber harrasment*.
 4. Pasal 29 terdapatnya unsur pidana mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi kekerasan dan/atau ancaman dan/atau menakut-nakuti seseorang. Pasal ini sesuai dengan bentuk perundungan siber jenis *cyber stalking*.
 5. Pasal 30 ayat (1) unsur pidana yang terdapat dalam pasal ini adalah melakukan akses sistem elektronik dan/atau komputer orang lain dengan apapun secara ilegal. Pasal dan ayat ini sesuai dengan bentuk perundungan siber jenis *impersonation* (meniru pribadi seseorang baik berbentuk gambar atau animasi dengan tujuan mengejek serta mengancam).

6. Pasal 32 ayat (2) dengan unsur pidana mentransfer atau memindahkan informasi elektronik dan/atau data elektronik ke sistem elektronik pihak lain yang tidak mempunyai hak. Pasal ini dapat diterapkan pada pelaku perundungan siber yang berbentuk *outing and trickery* (menyebarkan rahasia orang lain baik berupa foto, gambar, atau video seseorang dan tipu daya untuk mendapatkan informasi rahasia seseorang).

Kejahatan siber yang lain salah satunya adalah *hate speech* atau yang dikenal dengan ujaran kebencian, tindak pidana ini diatur dalam Kitab Undang-Undang Hukum Pidana dengan ketentuan lain di luar Kitab Undang-Undang Hukum Pidana. Bentuk dari ujaran kebencian ini adalah ;

1. Penghinaan;
2. Pencemaran nama baik;
3. Penistaan;
4. Perbuatan tidak menyenangkan;
5. Provokasi;
6. Menghasut;
7. Menyebarkan berita bohong;
8. Semua perbuatan atau tindakan yang berakibat terjadinya diskriminasi, penghilangan nyawa, kekerasan, dan/atau menimbulkan konflik sosial.

2. Upaya Pemerintah Dalam Mengatasi Perundungan Siber Di Indonesia

Indonesia adalah negara hukum, sebagaimana disebutkan dalam pasal 1 Undang-Undang Dasar Republik Indonesia Tahun 1945. Dan setiap

warga negara berhak untuk mendapatkan perlindungan dalam semua aspek kehidupan berbangsa dan bernegara.

Mochtar Kusumaatmadja berpendapat bahwa masalah-masalah dalam suatu masyarakat yang sedang membangun harus diatur oleh hukum, yang secara garis besar dapat dibagi menjadi dua golongan besar, yaitu ;

- a. Masalah-masalah yang langsung mengenai kehidupan pribadi seseorang dan erat hubungannya dengan kehidupan budaya dan spiritual masyarakat;
- b. Masalah-masalah yang bertalian dengan masyarakat dan kemajuan pada umumnya yang bersifat netral dilihat dari sudut kebudayaan.¹⁷

Dalam rangka mengatasi perundungan siber serta kejahatan-kejahatan siber lain di Indonesia, pemerintah Republik Indonesia memberikan kuasa kepada Kementerian Komunikasi dan Informatika RI untuk melakukan pembahasan hingga pengundangan revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) atau Undang-Undang RI Nomor 19 Tahun 2016 yang telah disetujui oleh Dewan Perwakilan Rakyat Republik Indonesia untuk diundangkan.

Karena diundangkan pada akhir November 2016 dengan suasana politik yang lumayan panas, UU ITE hasil revisi ini dianggap merupakan produk hukum untuk merespond atau bahkan mengekang penyampaian aspirasi rakyat.¹⁸ Revisi Undang-Undang Informasi dan Transaksi Elektronik tersebut secara resmi berlaku mulai 25 November 2016 bukan merupakan Undang-Undang Republik Indonesia yang baru apalagi dipergunakan oleh

¹⁷ Mochtar Kusumaatmadja, 2006, *Konsep-Konsep Hukum dalam Pembangunan*, PT. Alumni, Bandung, h. 30

¹⁸ Danrivanto, 2017, *Revolusi Cyberlaw Indonesia*, PT. Refika Aditama, Bandung, h. 93

pemerintah untuk suatu kepentingan politik atau untuk melindungi kepentingan pemerintah.

Dalam revisi Undang-Undang Informasi dan Transaksi Elektronik setidaknya ada lima poin penting dan baru yang menjadikan Undang-Undang Informasi dan Transaksi Elektronik 2016 ini relevan dengan pemenuhan rasa keadilan bagi masyarakat yang menggunakan dunia siber sebagai tempat untuk menyampaikan pendapatnya, yakni ;

- a. Menghindari penahanan serta merta dengan menurunkan pidana penjara dari 6 (enam) tahun menjadi 4 (empat) tahun;

Dengan penurunan ancaman ini, pihak pelapor dan terlapor mempunyai kedudukan yang sama sehingga dapat dibuktikan di pengadilan tentang siapa yang benar. Terlapor tidak perlu ditahan dahulu karena ancaman penjaranya di bawah 5 (lima) tahun.

- b. Menambahkan ketentuan mengenai *right to be forgotten* atau hak untuk dilupakan sebagaimana terdapat pada pasal 26;

Pada akhirnya penyelenggara sistem elektronik wajib menghapus informasi elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasar pada penetapan pengadilan dan menyediakan mekanismenya.

- c. Memberi perlindungan masyarakat dari konten negatif;

Dalam hal ini ada dua cara, yakni perlindungan dari segi pembatasan akses penyebaran dan perlindungan dari aspek pendidikan.

- d. Mengakomodir putusan Mahkamah Konstitusi Republik Indonesia dengan mengubah pengaturan tata cara intersepsi atau penyadapan, dari yang sebelumnya diatur dalam Peraturan Pemerintah menjadi diatur dalam Undang-Undang Republik Indonesia.
- e. Penegasan bahwa bukti hukum yang sah dari hasil intersepsi adalah intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan aparat penegak hukum.¹⁹

Sekarang di Indonesia sudah hadir hukum telekomunikasi yang pada dasarnya didorong dan ditujukan untuk tiga hal, yaitu :

1. penciptaan aspek pasar yang sebelumnya belum berlaku;
2. Pemisahan regulasi dari fungsi operasional;
3. Liberalisasi kegiatan tertentu yang awalnya dilarang, seperti kepemilikan asing.²⁰

Dari sini jelas sudah bahwa pemerintah tidak tinggal diam atas munculnya kasus perundungan siber di Indonesia, karena bagaimanapun juga keamanan semua warga negara dijamin oleh Undang-Undang Republik Indonesia yang mana hal itu juga merupakan hak asasi manusia yang dimiliki oleh semua warga negara sejak dilahirkan di dunia.

Adapun dalam penanganan kasus perundungan siber dibutuhkan juga bukti-bukti yang dapat dijadikan dasar dan secara umum bentuk dari alat bukti elektronik itu adalah informasi elektronik, dokumen elektronik serta keluaran komputer lainnya.

¹⁹ Ibid, h. 97

²⁰ Maskun, 2014, *Kejahatan Siber (Cyber Crime)*, Kencana Prenada Media Group, Jakarta, h. 25

Pasal 1 ayat (3) Undang-Undang Informasi dan Transaksi Elektronik menyebutkan bahwa informasi elektronik adalah : satu perkumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), *telegram*, *teleteks*, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Kemudian batasan dokumen elektronik sesuai dengan ketentuan pasal 1 ayat (14) Undang-Undang Informasi dan Transaksi Elektronik disebutkan bahwa setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektronik-magnetik, optikal atau sejenisnya; yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.²¹

Hukum pembuktian di Indonesia secara yuridis formal belum mengakomodasikan dokumen atau informasi elektronik sebagai alat bukti dalam penyelesaian di pengadilan²², kendati demikian sebenarnya di Indonesia sudah ada beberapa tindakan yang mengarah pada penggunaan serta pengakuan terhadap dokumen elektronik sebagai alat bukti yang sah.

²¹ Efa Laela Fakhriah, 2017, *Bukti Elektronik*, PT. Refika Aditama, Bandung, h. 25

²² Ibid, h. 24

3. Upaya Pencegahan Perundungan Siber

Kaspersky Lab dan iconKids & Youth pada tahun 2015 melakukan penelitian dan menemukan kalau perundungan siber menjadi sebuah ancaman yang sangat berbahaya dari apa yang diperkirakan.

Adapun hasil dari penelitian tersebut adalah 30% terjadi penurunan dalam proses belajar anak, 28% orang tua mengatakan anak-anak mereka mengalami depresi, 25% orang tua mengatakan pola tidur anak menjadi terganggu, 21% orang tua mengatakan bahwa perundungan siber menyebabkan mimpi buruk bagi anak. Selanjutnya 26% orang tua korban menyadari bahwa anak mereka mulai menghindari kontak dengan anak-anak lain dan 20% orang tua menemukan anak mereka mengidap anoreksia. Yang cukup mengkhawatirkan adalah angka statistik yang menunjukkan bahwa 20% dari anak-anak menyaksikan anak lain ditindas secara *online*, dan pada 7% kasus bahkan mereka ikut berpartisipasi dalam melakukan perundungan siber tersebut.²³

Penyebab terjadinya kejahatan menurut Separovic ada dua faktor yaitu ;

- a. Faktor personal, termasuk juga didalamnya adalah faktor biologis (umur, jenis kelamin, keadaan mental, dan lain-lain) serta faktor psikologis (agresivitas, kecerobohan, dan keterasingan).

²³ Rahmat Syah dan Istiana Hermawati, "Upaya Pencegahan Kasus Cyber Bullying Bagi Remaja Pengguna Media Sosial Di Indonesia", *Jurnal PKS*, No. 2, Vol. 17, 2018, h. 138-139

- b. Faktor situasional, seperti terjadinya situasi konflik, faktor tempat dan waktu.²⁴

Perundungan siber dapat dicegah dengan menggunakan Pre-emptif, Preventif, dan Represif (P2R). Pre-emptif merupakan upaya pencegahan dini kepada masyarakat melalui penyuluhan, sosialisasi, dan kampanye. Upaya tindak pre-emptif dilakukan oleh pihak kepolisian dalam mencegah perundungan siber dapat memaksimalkan cara-cara sebagai berikut ;

- 1) Memberikan penyuluhan kepada pelajar, mahasiswa, dan masyarakat tentang bahaya *bully* orang lain yang dilakukan secara kelompok maupun personal;
- 2) Menyesuaikan aturan terhadap pasal demi pasal dalam peraturan perundang-undangan Informasi dan Teknologi Elektronik (ITE) sebagai berikut :
 - a. Merespon tuntutan pelapor yang dapat mengakomodir aspirasi mereka.
 - b. Menawarkan pemuda/pemudi menjadi duta anti *cyber bullying*.
- 3) Melibatkan organisasi kemahasiswaan dan mengkampanyekan anti *cyber bullying*, selain itu juga dapat melibatkan organisasi sosial, organisasi pemuda, organisasi profesi, dan organisasi pelajar;
- 4) Melibatkan partai politik yang mampu memberikan pendidikan kepada kader pentingnya menggunakan media internet secara baik;
- 5) Menetapkan secara tegas para pelaku penyebar fitnah dan *cyber bulliet*;
- 6) Program bidang karya seni dan kreativitas berupa :

²⁴ Made Darma Weda, 1996, *Kriminologi*, PT. Raja Grafindo, Jakarta, h. 76

- a. Lomba membuat poster anti *bullying*
 - b. Lomba membuat artikel ilmiah anti *bullying*
- 7) Menerapkan sanksi dan hukuman minimal 5 tahun dan maksimal 10 tahun bagi pelaku *cyber bullying* di Indonesia.²⁵

Selanjutnya pihak kepolisian juga dapat melakukan tindakan preventif dengan melakukan strategi preventif yaitu memblokir akun-akun orang yang berkomentar secara *online* yang disitu mengandung unsur-unsur perundungan. Pemblokiran tersebut dapat dilakukan dalam rangka untuk mengurangi jumlah korban perundungan, pemblokiran dapat dilakukan dengan mengubah nomor, tidak memberikan nomor, melacak alamat *Internet Protocol* (IP), atau memblokir pelaku perundungan secara permanen dengan menghubungi pihak administrator dari berbagai website.

Kemudian tindakan represif juga dilakukan oleh pihak kepolisian dengan melakukan pengambilan tindakan dengan mendatangi secara langsung tempat kejadian perkara (TKP) untuk melakukan penangkapan serta melakukan tindakan penahanan terhadap pelaku perundungan siber, agar tidak berlarut-larut.

Selain pihak kepolisian, peran orang tua juga sangat penting dalam rangka upaya pencegahan perundungan siber, selama pengawasan dari orang tua intens kepada anak-anak yang menggunakan media internet maka akan sangat dapat menekan angka terjadinya perundungan siber.

²⁵ Abdul Sakban, 2019, *Pencegahan Cyber Bullying Di Indonesia*, Deepublish, Yogyakarta, h. 51-52

Hal-hal yang perlu diperhatikan dalam rangka pencegahan perundungan siber adalah sebagai berikut ;²⁶

a. Etika berinternet (*netiquette*)

Netiquette adalah kode etik yang mengatur cara para pengguna internet dalam beraktivitas di internet agar apa yang dilakukan tidak melanggar norma dan hukum yang berlaku sehingga fasilitas internet dapat digunakan sebagaimana mestinya tanpa ada pihak yang dirugikan karenanya.

b. Peran orang tua

Beberapa langkah orang tua dalam mengontrol penggunaan media internet oleh anaknya adalah :

1. Memberikan pendidikan agama yang lebih
2. Memberikan batasan waktu dalam menggunakan *handphone* dan waktu belajar
3. Mengontrol siapa teman pergaulan di media sosial
4. Memiliki akun media sosial milik anaknya untuk memudahkan pengecekan setiap waktu
5. Memberikan pemahaman pentingnya hidup bertoleransi di media internet
6. Memiliki sikap kritis terhadap akun-akun di media internet yang berindikasi ada pesan penghinaan, pengancaman, perundungan, dan ujaran kebencian.

c. Peran serta pihak kepolisian

²⁶ Ibid

Pihak kepolisian dapat melakukan sosialisasi dan kampanye anti *bullying*, selain itu juga dapat melakukan deteksi dini, pelaporan dan penanganan *bullying* baik dari individu maupun sistemik.

d. Peran organisasi sosial

Peran organisasi sosial dalam mencegah perundungan siber adalah dengan memperhatikan etika dalam berkomunikasi, menyampaikan berita positif di media sosial, saling mendukung satu sama lain, tidak saling menghujat antara satu dengan yang lain, bersikap empati terhadap sesama, dan bertoleransi.

4. Upaya Penanggulangan Perundungan Siber

Harga diri merupakan sebuah keyakinan individu tentang persepsi terhadap nilai pribadinya dan dipengaruhi oleh partisipasinya dalam dunia sosial dimana sering terjadi konflik interpersonal. Penelitian Melotti dan Brighi²⁷ menemukan remaja yang menjadi partisipan penelitiannya memiliki tingkat harga diri sedang ke tinggi, dan dengan persepsi harga diri yang tinggi di antara teman-teman sebaya dapat meningkatkan resiko menjadi pelaku perundungan siber.

Estimasi jumlah remaja yang mengalami perundungan siber di Indonesia sangat tinggi, survei global yang dilakukan oleh Ipsos terhadap 18.687 orang tua dari 24 negara termasuk Indonesia, menemukan bahwa 12% orang tua menyatakan bahwa anak mereka pernah mengalami perundungan

²⁷ Laras Bethari Ragasukmasuci dan Maria Goretti Adiyanti, "Kecenderungan Remaja Menjadi Pelaku Perundungan Siber : Kontribusi Harga Diri dan Kesepian", *Gajah Mada Journal Of Psychology*, No. 2, Vol. 5, 2019, h. 189

siber. Dan 60% diantaranya menyatakan bahwa anak-anak tersebut mengalami perundungan siber pada jejaring sosial.

Di Indonesia 14% orang tua yang menjadi responden survei ini menyatakan anak mereka pernah mengalami perundungan siber, dan 53% menyatakan mengetahui anak dikomunitasnya pernah mengalami perundungan siber.²⁸ Dari data tersebut kiranya sangat perlu adanya upaya penanggulangan terhadap perundungan siber karena apabila berlarut-larut maka dapat dimungkinkan akan semakin bertambah korban.

Perkembangan teknologi membawa dampak dalam dunia kejahatan, yang pada awalnya kejahatan hanya sebatas pencurian, penghinaan, pembunuhan, dan lain sebagainya yang semua itu sudah diatur dengan jelas dalam Kitab Undang-Undang Hukum Pidana (KUHP). Dan dengan perkembangan teknologi ini kejahatan juga semakin bertambah banyak dan dilakukan dengan tidak terbatas pada tempat dan waktu.

Kepastian hukum terkait perundungan siber di Indonesia sudah menenui titik terang dengan hadirnya beberapa peraturan perundangan yang diberlakukan, selain dalam menanggulangi tindak perundungan siber dengan menggunakan Kitab Undang-Undang Hukum Pidana (KUHP) yang secara khusus mengenai kekerasan diatur dalam Pasal 170, Pasal 336, dan Pasal 368 yang di dalam Kitab Undang-Undang Hukum Pidana (KUHP) kekerasan sering kali dihubungkan dengan ancaman yang dapat diasumsikan bahwa kekerasan dimaksud dalam Kitab Undang-Undang Hukum Pidana (KUHP)

²⁸ Machsun Rifauddin, "Fenomena Cyber Bullying Pada Remaja", *Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan Khizanah Al-Hikmah*, No. 1, Vol. 4, 2016, h. 39

adalah juga merupakan kekerasan dalam bentuk fisik maupun non fisik (ancaman kekerasan).

Dalam pasal 351 Kitab Undang-Undang Hukum Pidana (KUHP) penganiayaan merupakan tiap perbuatan yang dilakukan dengan kesengajaan serta ditujukan kepada orang lain serta mengakibatkan sakit atau luka (*elke opzettelijke veroorzaking van pijn of letsel*).²⁹ Artinya penganiayaan dimaksud bukan hanya sebatas kontak fisik dengan kata lain berpengaruh pada fisik serta dapat menyebabkan luka fisik.

Dalam menanggulangi perundungan siber juga dapat digunakan aturan lain di luar Kitab Undang-Undang Hukum Pidana (KUHP) seperti Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang sudah dirubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Secara spesifik Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjabarkan tentang aturan serta sanksi bagi pelaku kejahatan siber di Indonesia, maka dapat diambil konklusi bahwa untuk pelaku perundungan siber selain dapat dikenakan sanksi sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan juga dapat dikenakan sanksi sebagaimana diatur dalam Undang-Undang RI tentang ITE.

²⁹ Sudarto, 2009, *Hukum Pidana I*, Yayasan Sudarto Fakultas Hukum Undip, Semarang, h. 89