BAB III
PEMBLOKIRAN KONTEN MEDIA ELEKTRONIK

A. Istilah dan Pengertian Pemblokiran

1. Pengertian Pemblokiran

Meningkatnya penggunaan *internet* hari ini, telah berdampak pula pada terjadinya peningkatan dalam jumlah dan jenis kejahatan dunia maya. Dalam rangka antisipasi dan penindakan terhadap berbagai jenis tindak kejahatan dunia maya tersebut, negara-negara termasuk Indonesia telah melahirkan sejumlah kebijakan yang dimaksudkan untuk mengontrol dan mengawasi penggunaan *internet*, yang dibarengi dengan ancaman pemidanaan. Kebijakan ini khususnya yang terkait dengan konten *internet*. Setidaknya ada dua isu penting terkait dengan pengaturan konten *internet,* yaitu isu mengenai pemblokiran konten, serta isu pemidanaan terhadap pengguna akibat konten yang disebarluaskan.

Pemblokiran adalah suatu istilah yang membuat suatu akun, sebuah alamat/blok alamat IP, atau seseorang dicegah untuk melakukan penyutingan wikipedia.[1] Pemblokiran sering digunakan untuk menangani vandalism. Ada beberapa situasi lain dimana pemblokiran patut dilakukan. Dalam semua kasus, pemblokiran lebih bersifat mencegah dan bukan menghukum, dan hanya dilakukan untuk menghindari kerusakan wikipedia.[2] Blokir umumnya efektif selama 24 jam, kecuali untuk beberapa kasus dan biasanya akan dihapus jika kontributor tersebut setuju untuk menghentikan tidakan merusaknya. Semua user

[1] http://id.m.wikipedia.org/wikipedia:kebijakan_pemblokiran.diakses 16 November 2015,01.03

[2] http://id.m.wikipedia.org/wikipedia:kebijakan_pemblokiran.diakses 16 November 2015,01.03

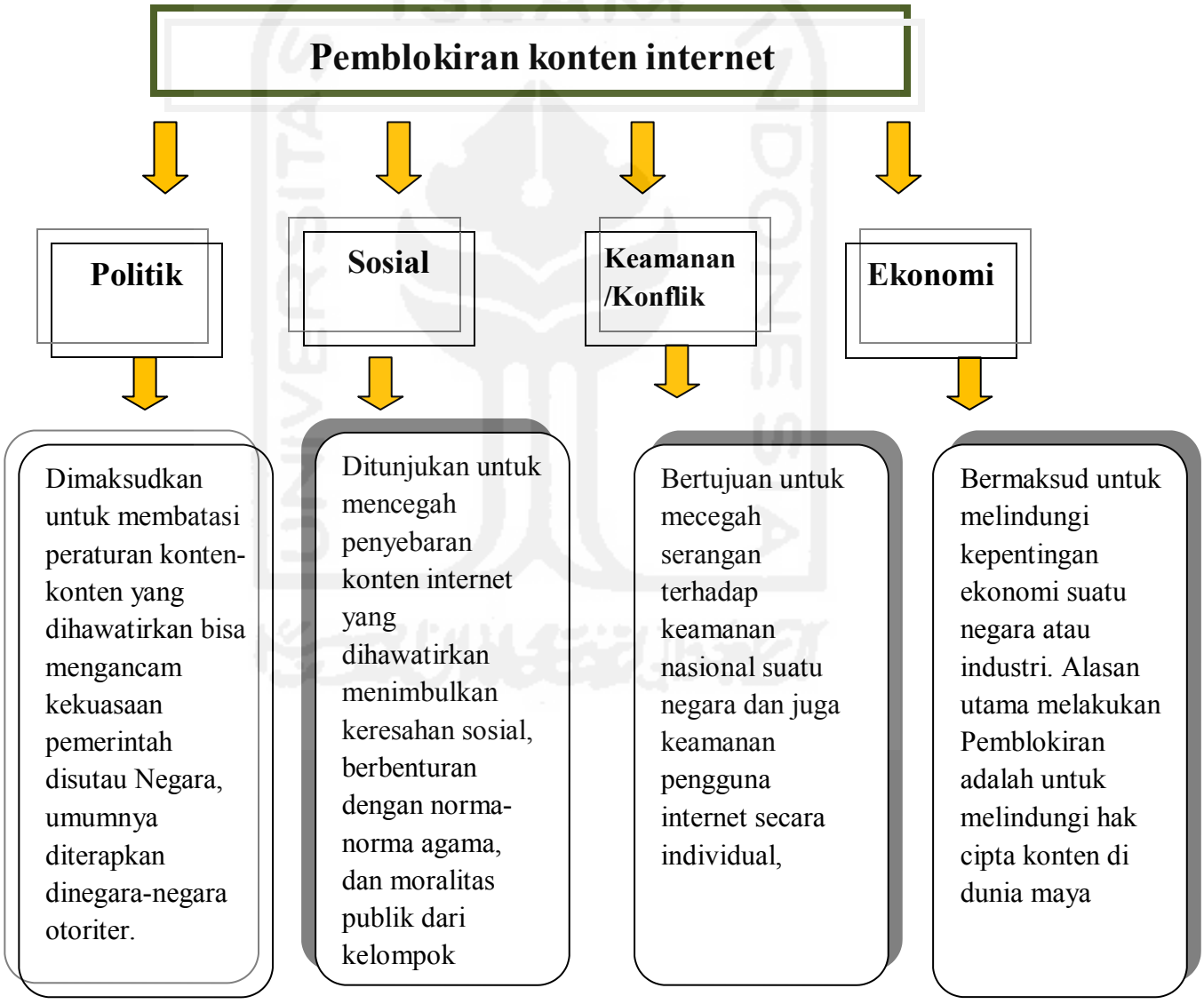
dapat mengirimkan permintaan pemblokiran melalui *warnet, gejet* dll. Tindakan pemblokiran segera akan dilakukan jika bukti-bukti pelangaran kebijakan bisa diberikan; tetapi, pengurus tidak diharuskan untuk menerapkan pemblokiran.

Teknik memblokir alamat dilakukan dengan cara melihat konfigurasi *router* tertentu yang digunakan untuk menolak akses ke *protokol internet* tertentu *(IP),* alamat dan/atau nama *domain*, atau layanan yang berjalan pada nomor *port* tertentu. Tindakan ini seperti yang dilakukan oleh beberapa negara yang menjalankan filter memblokir di *level gateway* internasional, dengan membatasi akses dari dalam negeri terhadap laman situs yang dianggap ilegal, seperti laman porno atau hak asasi manusia. Sementara teknik analisis isi mengacu kepada teknik yang digunakan untuk mengontrol akses ke informasi berbasis pada konten, seperti dimasukkannya kata kunci tertentu di laman situs atau alamat *URL*. Motede seperti ini sering menjadi sumber penyumbatan keliru atau tidak disengaja, yang terjadi sebagai akibat dari pemblokiran berbasis *IP* yang dijalankan pula, karena tidak biasa bagi banyak nama domain untuk berbagi alamat *IP* yang sama. Pemblokiran yang bertujuan untuk memblokir akses ke laman situs tertentu dengan memblokir alamat *IP*-nya, dapat mengakibatkan pemblokiran ribuan situs yang tidak terkait, karena berbagi *IP* yang sama. Lebih detailnya, mekanisme yang digunakan dalam pemblokiran sangat bervariasi, tergantung dari tujuan serta sumber daya yang tersedia untuk tindakan tersebut.

Hamper serupa dengan beragamnya yang digunakan dalam pemblokiran dari sisi dimensinya juga beranekaragam, tergantung pada kepentingan dan orentasi dari masing-masing negara yang melakukan praktek pemblokiran

tersebut. Secara umum dalam prakteknya di dunia, dikenal ada empat dimensi dalam pemblokiran konten, yang meliputi; dimensi politik, dimensi sosial, dimensi keamanan, dan dimensi ekonomi, pengertian dalam cakupan dari masing simensi tersebut dijelaskan oleh Robert Faris and Nart Villeneuve (2008), dalam figur berikut ini:[3]

Demensi pemblokiran konten *internet*. Gambar figur 1



[3] Robert Faris and Nart Villeneuve, Measuring Global Internet Filtering, dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied ... Op.Cit.*, hal. 5-26. Lihat juga Joanna Kulesza, *International Internet Law*, (London: Routledge, 2012), hal. 44-45.

Pemblokiran merupakan praktik yang mulai dilakukan untuk menutup akses pengguna terhadap konten yang tersaji di *internet.* Beberapa alasan umum praktik pemblokiran ini, antara lain terkait dengan kontrol terhadap ekspresi politik, baik berupa ekspresi yang dilakukan oleh warga negaranya, maupun sebagai upaya untuk menghalangi pengaruh dari luar negaranya terhadap praktik politik di dalam suatu negara. Selain itu, praktik pemblokiran sering pula didasarkan pada alasan yang terkait dengan pencegahan pornografi, perjudian dan kegiatan ilegal yang bermuataan negatif serta melindungi moralitas masyarakat.

Terkait dengan dua isu tersebut, terdapat beberapa persoalan yang dihadapi Indonesia saat ini. Misalnya, dalam tindakan pemblokiran konten *internet,* meski sejumlah peraturan perundang-undangan telah menjelaskan, namun Indonesia belum memiliki pengaturan yang memadai mengenai tata cara, termasuk komplain, terhadap tindakan pemblokiran konten. Peraturan perundang-undangan hanya mengatur mengenai kewenangan pemerintah untuk melakukan pemblokiran terhadap konten dengan muatan tertentu, seperti pornografi, penodaan agama, dan penyebaran kebencian. Akan tetapi aturan tersebut tidak menyediakan secara tegas mengenai ruang lingkup, batasan, mekanisme, serta upaya perlawanan dan komplain atas pemblokiran.

Sementara yang berkaitan dengan pemidanaan terhadap pengguna, selain berangkat dari argumentasi melindungi hak dan reputasi orang lain, yang kemudian melahirkan ancaman pidana penghinaan dan pencemaran nama baik, juga muncul pidana di *internet* dengan alasan penodaan agama dan penyebaran

kebencian berlatar SARA. Pengambil kebijakan di Indonesia, telah mengadopsi hampir seluruh tindak pidana dalam dunia *offline* (KUHP) ke dunia *online*, dengan ancaman hukuman yang lebih berat, alasannya berdampak lebih luas. Padahal, menyitir dari laporan Pelapor Khusus PBB untuk kebebasan berekspresi dan berpendapat, Frank La Rue, dikatakan, karena ciri unik dari *internet,* peraturan atau pembatasan yang mungkin dianggap sah dan seimbang bagi media tradisional (*offline*) sering tidak bisa diaplikasikan terhadap akses *internet.* La Rue mencontohkan, dalam kasus penghinaan atau pencemaran nama baik, dalam era *internet,* individu yang merasa nama baiknya tercemar bisa menggunakan hak jawabnya saat itu juga, sehingga sanksi pidana pencemaran nama baik lewat *internet* tidak perlu dijatuhkan.

Penggunaan hukum pidana secara sewenang-wenang untuk memberikan sanksi pada ekspresi yang sah melalui media *internet,* merupakan salah satu bentuk pembatasan yang paling keras pada hak, karena hal itu tidak hanya menciptakan efek menakut-nakuti *chilling effect*, tetapi juga menjurus pada pelanggaran hak asasi manusia yang lain. Bentuk-bentuk pelanggaran HAM lainnya misalnya terjadi ketika harus dilakukan penahanan terhadap orang yang dikenai sanksi pidana. Di dalam tahanan mereka potensial mengalami tindakan penyiksaan dan bentuk-bentuk tindakan atau hukuman lain yang merendahkan martabat manusia serta tidak manusiawi.

Tulisan ini akan mencoba menguaraikan berbagai problematika pengaturan dan praktik pembatasan *konten internet* yang terjadi di Indonesia, yang diaplikasikan dalam dua tindakan: pemblokiran *konten internet* dan ancaman

pemidanaan terhadap pengguna *internet*, khusus yang memiliki keterkaitan dengan jaminan perlindungan kebebasan sipil.

Kebijakan Pemblokiran atas beberapa situs negatif yang dilakukan pemerintah, menuai kritik dari Budiono, selaku pemimpin redaksi media *online* detik.com. Budiono pantas gusar. Iklan adalah pemasukan amat penting bagi media. Bagi media *online*, selain pendapatan lain-lain dari komisi penjualan tiket misalnya, iklan adalah andalan utama untuk hidup. Gangguan atas akses iklan gara-gara pemblokiran situs oleh pemerintah adalah hal yang merugikan secara bisnis, belum lagi kalau bicara soal ancaman terhadap kemerdekaan berekspresi sebagaimana dijamin oleh UUD 1945 hasil amandemen di Pasal 28.[4]

Pada tahun 2015, Pemerintah melakukan pemblokiran akses situs porno sebanyak 800 ribu situs porno terkait pornografi, tetapi masih terus muncul situs pornografi lainnya. Rudiantara mengatakan bila sekarang diblokir 100 situs maka besok dapat tumbuh 200 situs, begitu pula bila saat ini diblokir 500 situs maka bisa muncul 1.000 situs baru.[5]

Pada Tahun 2015 terkait kasus maraknya ISIS, Mentri Komunikasi dan Informatika Indonesia, Rudiantara membenarkan adanya pemblokiran situs-situs yang menyebarkan paham radikalisme. Pemblokiran dilakukan atas permintaan Badan Nasional Penanggulangan Terorisme guna mencegah maraknya paham

[4] Uni Zulfiani Lubis, op, Cit, hlm 2.

[5] http://www.harianterbit.com/m/nasional/12 Mei 2015/. Diakses tanggal 4 Juni 2015 jam 11:35

radikalisme dan terorisme. Setidaknya ada 22 situs yang diblokir oleh Kementrian Komunikasi dan Informatika.[6]

Kebijakan Pemblokiran atas situ-situs paham radikalisme, kembali menuai pro dan kontra. Salah satunya dari Komisioner Komisi Informasi Pusat, Yhannu Setyawan, beliau menganggap pemblokiran situs-situs radikal oleh Kementrian Komunikasi dan Informatika tidak sesuai prinsip demokrasi. Karena, pemblokiran tersebut dilakukan tanpa adanya penjelasan kepada publik, ataupun peringatan lebih dulu kepada pengelola situs, sehingga terkesan tertutup dan tidak transparan. Yhannu Setyawan juga menambahkan Kemenkominfo seharusnya menjelaskan kepada publik secara jelas dan transparan tentang bagaimana sesungguhnya mekanisme atau prosedur yang berlaku dalam menutup atau memblokir sebuah situs yang dianggap membahayakan masyarakat.[7]

Salah satu sumber pro dan kontra tersebut adalah terkait kebebasan berekspresi. Padahal pengaturan tentang kebebasan berekspresi dan berpendapat telah diatur dalam Undang-Undang Nomor 9 Tahun 1998 tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum. Menurut Undang-Undang Nomor 9 Tahun 1998 tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum. Pengertian tentang kemerdekaan menyampaikan pendapat adalah hak setiap warga negara untuk menyampaikan pikiran dengan lisan, tulisan dan sebagainya

[6] http://Kompas, pemblokiran Situs-situs radikal dianggap hidupkan kembali orde baru, nasional.kompas.com/1 April 2015/. Diakses tanggal 4 Juni 2015. jam 01.03

[7] *Ibid*

secara bebas dan bertanggung jawab sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.[8]

Saat ini, praktik pemblokiran merupakan praktik yang mulai dilakukan untuk menutup akses pengguna terhadap konten yang tersaji di *internet.* Beberapa alasan umum praktik pemblokiran ini, antara lain terkait dengan kontrol terhadap ekspresi politik, baik berupa ekspresi yang dilakukan oleh warga negaranya, maupun sebagai upaya untuk menghalangi pengaruh dari luar negaranya terhadap praktik politik di dalam suatu negara. Selain itu, praktik pemblokiran sering pula didasarkan pada alasan yang terkait dengan pencegahan pornografi serta melindungi moralitas masyarakat.

Walaupun begitu praktik pemblokiran ini telah jamak dilakukan melalui beberapa cara, yakni diantaranya melalui pencegahan pengguna mengakses laman tertentu, pemblokiran *Internet Protocol (IP),* ekstensi nama *domain*, dan penutupan suatu laman dari laman *server* yang ditempatinya.

Selain itu, pencegahan akses juga dilakukan dengan menerapkan sistem filter untuk memblok atau membuang laman yang mengandung kata-kata kunci tertentu. Dalam beberapa kasus, praktik ini dilakukan secara bervariasi, terdapat kasus-kasus dimana pemerintah memblok laman dan penyedia jasa, seperti dalam kasus pemblokiran *YouTube* dan pemblokiran mesin pencarian di Cina. Dalam beberapa hal praktik ini melibatkan pihak perantara pada saat penyedia jasa yang „dipaksa" melakukan pemblokiran pada penggunanya. Pola pemblokiran jenis ini berlangsung pula di Indonesia, perintah datang dari Kementerian Komunikasi dan

[8] Indonesia,Undang-Undang No.9 Tahun 1998, tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum, LN Tahun 1998 No 181, TLN Nomor 3789, Pasal 1.

Informatika kepada para penyedia layanan *(ISP)*. Beberapa contoh, seperti dalam kasus RIM di Indonesia kewajiban melakukan pemblokiran oleh penyedia jasa dimasukkan sebagai bagian dari perijinan beroperasi Khusus di Indonesia, sebetulnya belum adanya ketentuan yang secara detail mengatur mekanisme dan tata cara pemblokiran konten. Indonesia juga belum memiliki suatu badan khusus yang independen, yang diberikan mandat untuk melakukan pemblokiran konten *internet*. UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) terbatas hanya memberikan mandat yang terkait dengan konten-konten yang dianggap melawan hukum, namun lupa untuk memasukkan kebijakan kontrol terhadap konten.

Selanjutnya Masalah ini semakin diperparah dengan kurangnya transparansi dalam penerapan pembatasan-pembatasan tersebut, kurangnya panduan yang jelas yang bisa dijadikan landasan bagi para pengguna (*user*), dan ketiadaan mekanisme yang tepat untuk digunakan untuk melakukan banding terhadap keputusan yang diambil oleh penyedia layanan, yang akhirnya menyebabkan penyensoran konten yang dibuat oleh pengguna (*user-generated content*). Ini berarti konten *online* semakin ketat diatur dan disensor atas dasar kontrak privat dengan transparansi dan *accountable* yang amat terbatas.

Untuk dapat melakukan pembahasan yang mendalam mengenai masalah ini maka perlu dilakukan penelitian yang mendalam agar memberi gambaran yang jelas mengenai dasar kebijakan dalam penerapan tindakan pemblokiran terhadap informasi elektronik yang bermuatan sarana kejahatan pada saat ini. Selanjutnya

dibuat rumusan konsep kebijakan untuk tindakan pemblokiran dalam penanggulangan kejahatan berbasis konten media di masa mendatang.

Tahap formulasi, tahap penegakan hukum *in abstracto* oleh badan pembuat undang-undang, tahap disebut juga sebagai tahap kebijakan legislatif.[9] Akibat situasi itu, undang-undang ITE dikenal sebagai intrumen hukum yang mengatur segala aspek teknologi informasi dan kumunikasi di Indonesia, di dalamnya termuat ketentuan tentang informasi dan dokumen elektronik, transaksi elektronik, penyelenggaraan sertifikasi elektronik, serta hak kekayaan intelektual dan perlindungan pribadi, penyadapan, sangsi pidana dan sangsi administratif, serta banyak aspek-aspek lain yang berkenaan dengan para pelaku dan objek dalam dunia teknologi informasi den komunikasi. Jika ditijau secra keseluruhan, peraturan yang termaktub dalam UU ITE Nampak sangat dipaksakan karena memadukan banyak norma hukum yang pengaturannya dapat dilakukan dalam instrument hukum terpisah. Konsekuensinya, aspek-asepk peraturan dalam UU ITE Nampak kurang koheren atara satu dengan yang lainnya, terlepas dari itu banyaknya aspek yang berusaha diatur membuat pendalaman norma hukumnya menjadi dangkal dan berkutat pada tataran permukaannya saja.

2. Kebijakan Konten Internet Di Beberapa Yuridiksi

Intrumen hukum internasional yang mengatur masalah kejahatan mayantara *(cyber crime)* yang saat ini paling mendapat pengertian adalah *convenition no cyber crime* yang digagas Uni Eropa. Konvensi ini dibentuk dengan pertimbangan-pertimbangan, antara lain;

---

[9] Muladi, *Kapita Selekta Sistem Peradilan Pidana*, op.cit, hal.9.

a. Bahwa masyarakat internasional menyadari perlunya kerjasama antara negara dengan industri dalam memerangi kejahatan dunia maya dan adanya kebutuhan untuk melindungi kepentingan yang sah didalam penggunaan dan pembangunan teknologi informasi.
b. Konvensi saat ini diperlukan untuk meredam penyalagunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal.
c. Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatau kesesuaian antara pelaksanaan penegakan hukum dan hak asasi manusia sejalan denggan Konvensi Dewan Eropa untuk Perlindungan Hak Asasi Manusia dan Konvensi Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil.[10]

Konvernsi ini telah disepakati oleh Uni Eropa sebagai konvensi yang terbuka diaksesi oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan istrumen Hukum Internasional dan mengatasi kejahatan siber, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi.[11]

Dalam konvensi ini diatur pula hukum acara/formil bahwa negara anggota harus menerapkan undang-undang dan pendekatan-pendekatan lain yang diperlukan untuk membentuk kewenangan-kewenangan serta prosedur pelaksanaannya untuk tujuan penyidikan tindak pidana yang spesifik. Kewenangan dan prosedur yang dimaksud adalah pada tindak pidana sebagai mana yang disebutkan dalam jenis-jenis *cybercrime* diatas, tindak pidana yang

[10] Seri Perjajian Eropa 185- Konvensi tentang Tindak Pidana Telematika.23.XI.2001
[11] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*, Jakarta; Tatanusa, 2012, halaman. 79.

dilakukan melalui sistem komputer, dan pengumpulan bukti elektronik dari suatu tindak pidana (Pasal 14 CoC).

Dalam konvensi ini diatur pula mengenai kerjasama internasional yang mencakup ekstradisi, bantuan timbal balik dan informasi spontan, prosedur-prosedur tentang permintaan bantuan timbal balik dengan tidak adanya perjanjian-perjanjian internasional yang berlaku, dan kerahasiaan dan pembatasan penggunaan, sampai pada jangkauan yang selebar mungkin untuk tujuan penyidikan atau proses-proses mengenai pelanggaran-pelanggaran yang berhubungan dengan sistem dan data komputer, atau untuk pengumpulan data dalam bentuk elektronik dari sebuah pelanggaran (Pasal 23 CoC).

Salah satu dari berbagai isu sosialkultural dalam ranah *internet* adalah kebijakan konten, isu ini sering dibahas dari berbagai sudut pandang, mulai dari dari hak asasi manusia (kebebasan berekpresi dan kebebasan berkomunikasi), pemerintah dan teknologi. Paling tidak ada tiga kelompok konten yang mendapatkan perhatian[12] yakni:

a. Konten yang pengendaliannya memiliki konsensus global, termasuk dalam hal ini adalah pornografi anak-anak, penyebaran informasi yang mengandung pembenaran terhadap aksi genosida, dan aksi dari organisasi terorisme, yang seluruhnya dilarang berdasarkan hukum Internasional
b. Konten yang sensitif bagi Negara-negara, wilayah atau kelompok etnik tertentu terkait dengan nilai-nilai budaya dan agama di suatu negara.

[12] Lihat Jovan Kurbalija , *Sebuah pengantar tentang tata kelola internet*, APJII, hal 144

Komunikasi *online* yang telah semakin global memiliki tantangan bagi nilai-nilai lokal, budaya dan agama di berbagai kelompok masyarakat. Sebagian besar pengendalian konten di Negara-negara Timur Tengah dan Asia secara resmi dibenarkan demi melindungi nilai-nilai budaya tertentu, dan hal ini sering berarti bahwa akses terhadap *website* pornografi dan perjudian lokal dilarang.

c. Penyensoran Politis di *Internet.* Laporan *OpenNet Initiati*ve *(ONI)* pada tahun 2012 menunjukkan tidak kurang dari 32 Negara melakukan penyensoran terhadap konten yang bersifat politik.[13]

Saat ini di beberapa yurisdiksi, penerapan kebijakan konten dilakukan dengan banyaknya pilihan-pilihan hukum dan teknis misalnya: melalui pemblokiran pemerintah, sistem pemblokiran dan peringkat dari swasta, pemblokiran konten berdasarkan lokasi geografis**,** pengendalian konten melalui mesin pencarian, dan menggunakan Web 2.0 dimana pengguna bertindak sebagai *contributor***.**[14]

Pemain utama dalam ranah pengendalian konten biasanya adalah pemerintah yang menentukan konten apa yang harus dikontrol dan bagaimana caranya. Elemen umum bagi pemblokiran konten oleh pemerintah adalah pemerintah memiliki sebuah index *internet* terhadap website yang diblokir bagi warga negaranya.[15] Jika sebuah *website* termasuk dalam index *internet* ini, maka akses tidak akan diberikan. Secara teknis, pemblokiran ini menggunakan *protocol*

---

[13] http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-Country-list diakses 16 November 2015, 01.03.

[14] Op.Cit. Jovan Kurbalija

[15] *ibid*

Internet berbasis *router, proxy server* dan pengalihan arah sistem nama domain *(DNS)*.[16] Selain China, Arab Saudi dan Singapura, beberapa Negara lainnya semakin banyak mengadopsi praktik ini. Australia misalnya menerapkan system pemblokiran terhadap halaman-halaman nasional tertentu meskipun bukan halaman-halaman Internasional.[17]

B. Perinsip-Perinsip Tata Kelola Internet terkait Pemblokiran

Dalam perinsip-perinsip tatakelola *internet* pemblokiran dalam kebebasan berekspresi melindungi informasi, opini dan ide dalam segala bentuknya yang disebarkan melalui media apapun, tanpa memandang batas wilayah; hak kebebasan berekspresi mencakup tidak hanya hak untuk berbagi, namun juga untuk mencari dan menerima informasi.

Internet adalah benda publik yang telah menjadi amat penting untuk pelaksanaan dan dinikmatinya hak kebebasan berekspresi secara efektif. Perinsip-perinsip *Internet* di antaranya[18];

1. *Internet* menungkinkan para individu untuk mencari, menerima, dan menyebarkan informasi dan gagasan tentang semua hal secara cepat dan murah melampui batas-batas kebangsaan. Dengan meluasnya kapasitas individu dalam menikmati hak mereka terhadap kebiasan berekspresi dan berpendapat, yang merupakan pendukung bagi hak asasi manusia, *internet* membantu pembangunan politik, ekonomi, dan social, dan berkontribusi bagi perkembangan umut manusia secara keseluruhan.

---

[16] *ibid*
[17] *ibid*
[18] http://128828_BUKUSAKU-kebebasan_berekspresi_di_internet.pdf.diakses12 Desember 2015.09:35

2. *Internet* telah menjadi sebuah alat komunikasi yang digunakan banyak individu untuk menyalurkan hak kebebasan berpendapat dan berekspresi, melalui pasal 19 di dalam konvenan (kesepakatan) internasional tentang Hak Sipil dan Politik. Pasal 19 pada kesempatan tersebut tertulis sebagai berikut;

a) Semua orang mempunyai hak untuk berpendapat tanpa adanya campur tangan (pihak lain)

b) Semua orang mempunyai hak kebebasan berpendapat; hak ini meliputi kebebasan untuk mencari, menerima dan menyebar-kan informasi dan ide-ide mengenai apapun tanpa batasan-batasan, baik secara lisan, tertulis atau cetak, dalam bentuk seni, atau melalui media pilihannya yang lain.

c) Penggunaan hak tersebut mempunyai kewajiban dan tanggungjawab khusus. Hal tersebut bisa menjadi subyek dari pembatasan-pembatasan tertentu, tapi semua pembatasan ini haruslah dengan hukum dan dilakukan karena benar-benar penting; a) Sebagai penghargaan bagi hak atau reputasi dari pihak lain; b) sebagai perlindungan keamanan nasional atau ketertiban umum, atau kesehatan atau moral masyarakat.

3. Semua orang mempunyai hak untuk mengekspresikan diri melalui media apapun. Pasal 19 Deklarasi Universal Hak Asasi Manusia dan Pasal 19 Kovenandan mengakomodasi perkembangan teknologi dimasa mendatang, dimana para individu dapat menggunakan hak atas kebebasan

berekspresi. Kerangka kerja dari hukum hak asasi manusia internasional tetap sesuai sampai sekarang dan bisa diaplikasikan untuk teknologi komunikasi yang baruseperti *internet.*

4. Hak atas kebebasan berpendapat dan berekspresi adalah hak yang sangat fundamental baik bagi hak-hak lain; termasuk hak ekonomi, sosial, dan budaya, seperti hak atas pendidikan dan hak untuk berperanserta dalam kehidupan budaya dan menikmati keuntungan perkembangan ilmu pengetahuan dan penerapannya, dan hak sipil dan politik; seperti hak atas kebebasan berorganisasi dan berkumpul.
5. Pembatasan pada arus informasi melalui *internet* beberapa keadaan tertentu yang dijabarkan oleh hukum hak asasi manusia internasional. Jaminan penuh bagi hak atas kebebasan berekspresi harus menjadi norma, dan pembatasan apapun dianggap sebagai sebuah pengecualian.
6. Penyedian akses *internet* kepada semua orang dengan seminimal mungkin pembatasan terhadap konten *internet* haruslah menjadi prioritas semua negara. Resolusi PBB telah menghimbau semua negara untuk memajukan dan memfasilitasi akses kepada *internet* dan kerjasama internasional yang ditujukan pada pembangunan media dan informasi serta fasilitas-fasilitas komunikasi di semua negara.

7. Peningkatan kesadaran dan usaha-usaha pendidikan guna memajukan kemampuan setiap orang dalam menggunakan *internet* secara mandiri dan bertanggungjawab perlu dikembangkan.[19]

Pelaksanaan hak kebebasan berekspresi dapat dibatasi hanya atas dasar yang telah ditentukan dalam hukum internasional, termasuk untuk melindungi hak orang lain. Hak-hak orang lain mencakup perlindungan hak atas properti dan khususnya hak cipta. Tidak ada pembatasan kebebasan berekspresi atas dasar proteksi hak pihak lain, termasuk hak cipta, yang dapat diterapkan, kecuali jika Negara bagian dapat menunjukkan bahwa pembatasan tersebut ditentukan oleh hukum dan diperlukan dalam masyarakat yang demokratis untuk melindungi kepentingan kepentingan tersebut. Beban untuk menunjukkan validitas pembatasan tersebut ditanggung oleh Negara bagian.

1. Ditentukan oleh hukum berarti hukum tersebut harus dapat diakses, tidak bermakna ganda, ditulis dengan makna sempit dan dengan presisi yang selayaknya sehingga memungkinkan individu untuk menilai apakah suatu tindakan tertentu tidak sah secara hukum atau sebaliknya.
2. Hukum tersebut harus memberikan penjagaan yang cukup dari penyalahgunaan. Sebagai salah satu aspek supremasi hukum, hukum tersebut harus mencakup adanya pemeriksaan yang segera, penuh danefektif atas validitas suatu pembatasan yang dilaksanakan oleh suatu pengadilan, tribunal atau badan peradilan independen lainnya.

[19] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*, Jakarta; Tatanusa, 2012

3. Pembatasan apapun terhadap kebebasan berekspresi yang berusaha dijustifikasi oleh Negara bagian atas dasar perlindungan kepentingan hak cipta harus memiliki tujuan yang murni dan dampak yang dapat dibuktikan *(demonstrable effect)*, atas dasar bukti independen, untuk melindungi tujuan-tujuan yang dimaksudkan untuk dicapai dengan hak cipta, sebagaimana dinyatakan dalam Pembukaan ini.
4. Pembatasan kebebasan berekspresi adalah proporsional dalam suatu masyarakat demokratis hanya jika:
    a. Pembatasan tersebut adalah cara yang mengandung pembatasan paling minimal untuk melindungi kepentingan tersebut; dan
    b. Pembatasan tersebut sesuai dengan prinsip-prinsip demokratis.

Negara bagian tidak hanya wajib menahan diri dari mengintervensi kebebasan berekspresi, namun juga berada di bawah kewajiban positif untuk melindungi kebebasan berekspresi dari intervensi pihak-pihak privat.

Belum lama ini, *Trust+positif* yang dikelola oleh Kemenkominfo menginstruksikan penyedia jasa layanan *internet* untuk memblokir Vimeo, sebuah situs berbagi video yang masuk ke dalam daftar negatif. Masuknya vimeo ke dalam daftar tersebut oleh argumentasi bahwa Vimeo mengandung konten-konten yang bermuatan pornografi. Seperti halnya tindakan pemblokiran berlebihan yang dilakukan atas atensi dari Kominfo sebelumnya, pemblokiran terhadap Vimeo kontan memicu kontroversi di masyarakat, yang menilai Kominfo tidak cermat dalam mengambil tindakan. Kominfo tidak melakukan telah secara mendalam mengenai muatan konten vimeo dan tidak mempertimbangan implikasi negatif

apabila vimeo diblokir. Sementara Beberapa situs yang dibuat untuk mengedarkan konten pornografi justru dibiarkan saja oleh Kominfo, sedangkan vimeo yang banyak digunakan pengguna *internet* untuk berbagi karya cipta visual justru diblokir. Masyarakat sendiri banyak berpendapat bahwa kemanfaatan yang mereka peroleh melalui vimeo justru lebih banyak daripada kerugiannya. vimeo menjadi salah satu media berbagi yang efektif, dengan ribuan jenis konten yang termuat di dalamnya. Konten pornografi hanyalah satu konten negatif dari ribuan konten positif bermanfaat lainnya. Sehingga, pemblokiran terhadap vimeo dinilai sebagai solusi yang tidak proporsional dengan masalah yang ingin dipecahkan.

Selama proses pembahasan RUU ITE, isu mengenai pemblokiran sebenarnya sangat terkait dengan proses penegakan hukum, apabila terjadi pelanggaran terhadap perbuatan yang dilarang menurut UU ITE. Menurut aparat penegak hukum, jika tindakan pemblokiran tidak dilakukan, pelaku dapat saja mengubah atau menghilangkan barang bukti kejahatan. Artinya, tindakan pemblokiran dimaknai seperti halnya tindakan penyitaan terhadap barang bukti kejahatan. Dalam praktiknya, pemblokiran konten *internet* yang dilakukan oleh penyedia layanan *internet*, atas perintah dari Kemenkominfo melalui program *Trust+Positif,* ditujukan terhadap konten yang dinilai mengandung muatan negatif menurut pemahaman pemerintah. Masalahnya, UU ITE sendiri tidak secara jelas mengatur kategorisasi konten yang dapat diblokir, dengan alasan apa, dilakukan oleh institusi negara yang mana, bagaimana prosedurnya, apa mekanisme komplain yang tersedia, dan prosedur pemulihan yang disediakan.

Pemblokiran terhadap konten *internet* memang boleh dilakukan oleh negara, sebagai bentuk pembatasan terhadap hak atas kemerdekaan berekspresi yang memang boleh dibatasi. Namun demikian dalam pembatasannya musti mengacu pada kaidah dan prinsip pembatasan sebagaimana diatur oleh Konstitusi maupun hukum internasional hak asasi manusia. ketika suatu negara akan melakukan tindakan pemblokiran terhadap konten *internet*, maka aspek-aspek yang musti diperhatikan adalah sebagai berikut:

no	Aspek	Penjelasan
1	Tujuan	Langkah paling awal dalam mengambil tindakan pemblokiran adalah merumuskan tujuan dari dilaksanakannya tindakan tersebut
2	Pernyataan resmi tentang tindakan yang akan diambil	Dilatarbelakang tujuan pada nomor 1, maka perlu dibuat peryataan bahwa pemerintah merasa perlu mengambil tindakan berupa pemblokiran terhadap konten yang bermutan negatif
3	Penjelasan khusus cara pemblokiran yang dilakukan	Aspek ini mengakomodasi perlunya negara memastikan setiap orang dapat mengerti hukum dan pendapat memeriksa bahwa tindakan pembatasan tidak dilakukan sewenang-wenang,
4	Dasar justifikasi dari tindakan pemblokiran	Pada bagian ini, dicantumkan hal yang menjustifi -kasi dilakukannya tindakan pembatasan. Dalam konteks ini, baik hukum internasional, hukum nasional, konvensi yang diterima masyarakat secara luas, nilai dan norma yang berlaku, dapat dijadikan dasar justifikasi. Misalnya, keamanan nasional atau ketertiban umum atau moral umum sebagai-mana diatur ketentuan Pasal 19 ayat (3) Kovenan tentang hak-hak Sipil dan Politik

5	Elaborasi mengenai permasalahan yang sedang terjadi dan mekanisme pelaksanaan pembatasan tersebut	Dalam aspek ini, perlu diurutkan secara lengkap, prosedur pelaksana dari pilihan tindakan pemeritah pada nomor 2. Aspek ini merupakan wujud transp-aransi kepada masyarakat dalam rangka mendorong adanya pengawasan untuk mencegah kesewenang-wenang pemerintah. Misal, menjelaskan bahwa apabila suatu situs web diblokir, penggun *internet* akan menerima pesan: i) menujukkan mengapa pemblokiran ini terjadi dan hukum apa yang dijadikan dasar untuk melakukan tindakan itu, ii) menyertakan penjelasan mengenai bagaimana pengguna *internet* dapat melaporkan masalah dan menerima pesan.

Praktik di beberapa negara menunjukkan setiap kali terjadi pemblokiran terhadap halaman *web* atau situs tertentu, pemerintah akan mendahuluinya dengan peringatan. Jika tidak ditindaklanjuti, pemerintah melalui otoritas yang berwenang akan memblokir halaman *web* atau situs yang bersangkutan dengan mencatumkan pernyataan jelas bahwa halaman yang bersangkutan diblokir. Uraian alasan yang melatarbelakangi pemblokiran, dan memberitahukan mekanisme banding yang dapat ditempuh pemilik konten dalam hal yang bersangkutan merasa keberatan atas tindakan tersebut. Beberapa ahli mengusulkan mekanisme peradilan sebagai wadah bagi para pemilik atau penyedia jasa konten untuk dapat mengajukan banding atas tindakan yang dilakukan pemerintah. Selain itu juga berkembang praktik mediasi *online* dan *arbitrase online* yang akrab disebut dengan *Online Dispute Resolution* (ODR). Alternatif penyelesaian tersebut pada dasarnya sama dengan konsep yang biasa dikenal masyarakat, hanya saja lembaga ini khusus menyelesaikan sengketa *online*. Sebagaimana praktik mediasi dan *arbitrase* pada umumnya, penyelesaian sengketa dengan metode ini cenderung cepat dan lebih mampu mengakomodasi kebutuan para pihak.

Secara umum, kerangka hukum tentang pemblokiran dapat dibagi menjadi dua aturan. Aturan normatif tentang jenis konten yang dilarang dan jenis mekanisme kontrol yang perlu diterapkan terhadapnya. Akan tetapi sedapat mungkin pemblokiran konten diposisikan sebagai langkah terakhir setelah melalui tahap pemberitahuan tentang adanya konten terlarang. Pemberitahuan ini dilakukan baik terhadap pihak pemilik atau penyedia konten dan terhadap para pengguna *internet*. Konten yang dilarang dapat ditandai sebagai rambu-rambu pengguna *internet* untuk memutuskan apakah konten tersebut akan dilihatnya atau tidak.

Mekanisme yang demikian akan mendorong pencerdasan dan pendewasaan para pengguna *internet* dalam menyikapi berbagai konten *internet*, khususnya dalam menentukan konten mana yang baik dan mana yang buruk bagi dirinya. Mekanisme yang demikian juga bertujuan untuk menghindari pemblokiran yang salah sasaran, mengingat mekanisme blokir yang digunakan di masa sekarang masih didasarkan pada kata kunci atau *key words*. Dalam mekanisme ini, konten *internet* yang mengandung kata kunci terlarang akan otomatis tidak dapat diakses oleh pengguna. Padahal, beberapa konten dengan kata kunci tersebut justru tidak bermuatan hal negatif sama sekali. Di sisi lain, beberapa konten negatif dan tidak baik untuk dikonsumsi oleh orang justru tidak menggunakan kata kunci tersebut.

C. Pihak-pihak yang Bisa Melakukan Pemblokiran

Sebelum membicarakan lebih jauh mengenai praktik-praktik pemblokiran terhadap konten *internet* yang terjadi di Indonesia, terlebih dahulu kita samakan

pengertian terlebih dahulu mengenai pemblokiran konten *internet* adalah istilah yang mengacu pada teknik kontrol yang dikenakan kepada akses informasi di *internet*. Teknik ini dapat dibagi menjadi dua teknik yang terpisah: (i) teknik alamat; dan (ii) teknik analisis isi (konten).[20] Secara umum pemblokiran konten *internet* dimaknai sebagai bentuk pengaturan melalui arsitektur teknologi. Arsitektur teknologi dibuat agar konten-konten terlarang tak dapat diakses oleh publik. Model tindakan seperti ini dinilai sebagai moda regulasi yang paling efektif untuk *internet,* sebab moda regulasi tradisional tidak bisa sepenuhnya cocok untuk medium yang bersifat lintas batas.

18 Lihat Ronald J. Deibert dan N. Villeneuve, Firewalls and Power: An O Teknik memblokir alamat dilakukan dengan cara melihat konfigurasi *router* tertentu yang digunakan untuk menolak akses ke *protokol internet* tertentu *(IP),* alamat dan/atau nama domain, atau layanan yang berjalan pada nomor *portokol internet* tertentu. Tindakan ini seperti yang dilakukan oleh beberapa negara yang menjalankan filter memblokir di *level gateway* internasional, dengan membatasi akses dari dalam negeri terhadap laman situs yang dianggap ilegal, seperti laman porno atau hak asasi manusia. Sementara teknik analisis isi mengacu kepada teknik yang digunakan untuk mengontrol akses ke informasi berbasis pada konten, seperti dimasukkannya kata kunci tertentu di laman situs atau alamat *URL.* Motede seperti ini sering menjadi sumber penyumbatan keliru atau tidak disengaja, yang terjadi sebagai akibat dari pemblokiran berbasis *IP* yang dijalankan pula, karena tidak biasa bagi banyak nama domain untuk berbagi

[20] Lihat Ronald J. Deibert dan N. Villeneuve, Firewalls and Power: An Overview of Global State Censorship of The Internet, dalam M. Klang dan A. Murray (eds.), *Human Rights in the Digital Age*, (London: Cavendish Publishing: 2004).

alamat *IP* yang sama. Pemblokiran yang bertujuan untuk memblokir akses ke laman situs tertentu dengan memblokir alamat *IP*-nya, dapat mengakibatkan pemblokiran ribuan situs yang tidak terkait, karena berbagi *IP* yang sama. Secara garis besar, tindakan pemblokiran dapat dikategorikan menjadi tiga:[21]

1. Pemblokiran terbuka (inklusi): model pemblokiran ini mengijinkan pengguna untuk mengakses daftar pendek situs yang disetujui, dikenal sebagai „daftar putih", sedangkan konten lainnya diblokir.
2. Pemblokiran dengan pengecualian: model ini membatasi akses pengguna dengan memblokir situs yang terdaftar pada „daftar hitam", sedangkan semua konten lainnya diijinkan.
3. Analisis isi: model ini membatasi akses pengguna dengan melakuan analisis secara dinamis terhadap konten laman situs dan memblokir situs-situs yang mengandung kata kunci dilarang, grafis atau kriteria tertentu lainnya.

Lebih detailnya, mekanisme yang digunakan dalam pemblokiran sangat bervariasi, tergantung dari tujuan serta sumber daya yang tersedia untuk tindakan tersebut. Pilihan mekanisme juga sangat tergantung pada kemampuan dari institusi yang meminta dilakukannya pemblokiran, khususnya sejauhmana mereka mereka memiliki akses kepada pihak-pihak yang dapat mewujudkan keinginan mereka. Pertimbangan lainnya termasuk jumlah kesalahan yang dapat diterima, apakah pemblokiran harus dilakukan secara terbuka atau terselubung, serta bagaimana itu bisa diandalkan. Secara detail Steven J. Murdoch and Ross

[21] Lihat Ronald J. Deibert, *The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace*, dalam Andrew Chadwick dan Philip N. Howard, *Handbook of Internet Politics*, (London: Routledge, 2009), hal. 324-325.

Anderson (2008) menjelaskan sejumlah mekanisme yang digunakan dalam pemblokiran berikut ini:[22]

1.Mekanisme *Header* TCP/IP Pemblokiran

Mekanisme ini dilakukan dengan cara inspeksi paket *header* yang umumnya berlokasi di alamat *IP* tujuan oleh *router* ketika seseorang berusaha mengakses suatu situs. Hal ini dimaksudkan guna mencegah suatu alamat *IP* tertentu agar tidak dapat diakses oleh pengguna, maka *router* dikonfigurasi untuk memblokir paket tujuan yang masuk dalam daftar hitam pemblokiran. Teknik ini memiliki kelemahan karena setiap *host* umumnya menyediakan banyak layanan situs *web* dan *email*, sehingga semua layanan yang tersedia oleh *host* tersebut bia turut terblokir. Oleh karena itu, untuk meningkatkan presisi blokir agar layanan lain tidak terblokir, biasanya dilakukan dengan memasukkan nomor *internet portokol* dalam daftar hitam tambahan.[23]

2.Mekanisme *Content* TCP/IP Pemblokiran

Pemblokiran metode ini hanya dilakukkan terhadap konten yang ilegal. Akan tetapi, *router* hanya mampu menginspeksi *header* pada paket, sehingga membutuhkan perangkat keras khusus untuk bisa menginspeksi seluruh konten dalam *traffick*. Namun perangkat lunak seperti itu umumnya tak mampu bereaksi cepat untuk melakukan pemblokiran jika menemukan konten yang melanggar hukum. Dengan demikian, membutuhkan perangkat lain lagi untuk bisa melakukan blokir terhadap konten ilegal yang ditemukan oleh perangkat inspeksi

[22]Steven J. Murdoch and Ross Anderson, *Tools and Technology of Internet Filtering*, dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, (The President and Fellows of Harvard College, 2008), hal. 57-65.

[23] *ibid*

tersebut. Selain itu, paket sendiri memiliki keterbatasan volume sehingga suatu konten umumnya dipecah dalam beberapa paket. Akibatnya, pada umumnya hanya bagian-bagian dari konten ilegal saja yang terdeteksi dan terblokir.[24] Selain itu, umumnya kata kunci juga terpecah dalam berbagai paket sehingga ada bagian konten ilegal yang tak terdeteksi karena tidak ada kata kunci pada paket tersebut.

3.Mekanisme DNS *Tampering*

Mekanisme ini dilakukan dengan cara memblokir seluruh alamat domain yang dimasukkan dalam daftar hitam. Caranya adalah memasukkan daftar hitam alamat domain pada *server DNS,* sehingga jika ada permintaan untuk mengunjungi nama domain yang dimaksud akan muncul pesan „*error*" atau „*no answer*". Teknik seperti ini sangat praktis namun berakibat blokir terhadap seluruh alamat domain, bukan hanya laman tertentu yang mengandung konten ilegal.[25]

4.Mekanisme HTTP *Proxy* Pemblokiran

Mekanisme ini bisa dilakukan dengan cara mengarahkan pengguna mengakses suatu situs *web* melalui *server proxy. Server proxy* menyimpan suatu laman pada sebuah *cache*, sehingga bisa diakses lebih cepat dan menghemat *bandwith.* Proxy bisa berfungsi untuk memblokir situs *web* karena *proxy* bisa memutuskan apakah permintaan untuk mengakses suatu situs bisa diterima atau ditolak. Kelebihan pemblokiran *proxy* adalah bisa memfilter perhalaman *web,* tidak harus memblokir seluruh alamat domain atau alamat *IP.* Dengan demikian,

---

[24]Steven J. Murdoch and Ross Anderson, *Tools and Technology of Internet Filtering,* dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, (The President and Fellows of Harvard College, 2008), hal. 57-65.

[25] *ibid*

pemblokiran dengan *HTPP Proxy* umumnya lebih presisi dibanding dua teknik sebelumnya.[26]

5.Mekansime *Hybrid* TCP/IP dan HTTP *Proxy*

Mekanisme ini dilakukan dengan cara membuat daftar alamat *IP* situs-situs yang memuat konten terlarang namun tidak memblokir data yang mengalir dari dan ke *server*, melainkan mengarahkan *traffick* ke *HTTP Proxy*. Pada *HTT Proxy* tersebut seluruh isi situs web diinspeksi dan jika menemukan konten terlarang langsung diblokir.[27]

6.Mekanisme *Denial-of-Service* (DoS)

Mekanisme ini dilakukan ketika pihak yang akan melakukan pemblokiran tidak memiliki kewenangan (atau akses ke infrastruktur jaringan) untuk menambahkan mekanisme pemblokiran konvensional. Caranya dengan mengakses sebuah situs secara otomatis melalui jaringan super cepat sehingga situs tersebut kelebihan kapasitas dan tidak bisa diakses.[28]

7.Mekanisme *Domain Deregistration*

Mekanisme ini dapat dilakukan terhadap situs dengan alamat domain kode negara *(ccTLDs)* dimana negara mengelola nama domain tersebut. Dengan menderegistrasi suatu nama domain, maka sub-sub domain yang berada dibawahnya akan terhapus juga secara otomatis.[29]

---

[26] Steven J. Murdoch and Ross Anderson, *Tools and Technology of Internet Filtering,* dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, (The President and Fellows of Harvard College, 2008), hal. 57-65.

[27] *Ibid*

[28] *Ibid*

[29] *Ibid*

8.Mekanisme *Server Take Down*

Mekanisme ini dilakukan jika suatu situs yang dianggap ilegal berlokasi pada *server* yang ada di dalam negeri. Pemerintah bisa meminta operator untuk menutup server suatu situs sehingga tidak bisa diakses oleh siapapun.[30]

9.Mekanisme *Surveillance*

Mekanisme ini digunakan dengan cara memonitor situs-situs yang dikunjungi pengguna. Jika pengguna tersebut mengakses konten terlarang, atau berusaha untuk mengaksesnya, lalu yang bersangkutan ditindak baik secara legal maupun *extralegal*. *Surveillance* umumnya dipakai sebagai pelengkap pemblokiran konvensional. *Surveillance* bertujuan menimbulkan efek ketakutan karena membuat pengguna *internet* merasa dimata-matai sehingga tidak berani mengakses situs terlarang.[31]

10. Mekanisme *Social Techniques*

Mekanisme ini dilakukan dengan cara membuat mekanisme sosial untuk membuat orang enggan mengakses konten terlarang. Misalnya menempatkan komputer di tempat yang terbuka seperti ruang keluarga, warung *internet* tanpa sekat, penempatan komputer di perpusataan dengan sekat kaca dan sebagainya. Selain itu bisa juga menempatkan *CCTV* di tempat-tempat mengakses *internet.*

---

[30]Steven J. Murdoch and Ross Anderson, *Tools and Technology of Internet Filtering,* dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, (The President and Fellows of Harvard College, 2008), hal. 57-65.

[31] *Ibid*

Metode lainnya bisa dengan kewajiban registrasi dengan kartu identitas asli sehingga pengguna merasa dimonitor.[32]

Hampir serupa dengan beragamnya teknik dan mekanisme yang digunakan dalam pemblokiran dari sisi dimensinya juga beranekaragam, tergantung pada kepentingan dan orientasi dari masing-masing negara yang melakukan praktik pemblokiran tersebut. Secara umum dalam praktiknya di dunia, dikenal ada empat dimensi dalam pemblokiran konten, yang meliputi: dimensi politik, dimensi sosial, dimensi keamanan, dan dimensi ekonomi. Dan yang bisa melakukan pemblokiran *ISP* karena untuk bisa *connect* ke *internet* setiap orang menggunakan jasa *ISP*.

Pihak yang berwenang melakukan pemblokiran adalah Undang-Undang Dasar Pasal 28 A - J tahun 1945 tentang HAM dan juga Pasal 19 Kovenan Hak Sipil dan Politik, Undang-Undang Nomor 28 tahun 2014 tentang Hak Cipta, Undang-Undang Nomor 44 tahun 2008 tentang ponografi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Traksaksi Elektronik (ITE), Peraturan Menteri Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif. dengan meyerahkan kepada Jasa penyedia pemblokiran sesuai Peraturan Menkominfo Nomer 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, pada Bab IV Peran Mayarakat dan Pemerintah, di pasal 7 disebutkan bahwa;

---

[32]Steven J. Murdoch and Ross Anderson, *Tools and Technology of Internet Filtering,* dalam Ronald Deibert, John Palfrey, Rafal Rohozinski, dan Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, (The President and Fellows of Harvard College, 2008), hal. 57-65.

1) *Masyarakat dapat ikut serta menyediakan layanan pemblokiran dengan memuat paling sedikit situs-situs dalam TRUST+Positif.*
2) *Layanan pemblokiran sebagaimana dimaksud pada ayat (1) dilakukan oleh Penyedia Layanan Pemblokiran.*
3) *Penyedia Layanan Pemblokiran harus memiliki kriteria sekurang kurangnya:*
   a. *terdaftar sebagai Penyelenggara Sistem Elektronik;*
   b. *berbadan hukum Indonesia;*
   c. *memiliki dan/atau menggunakan data center di Indonesia; dan*
   d. *memiliki prosedur operasi yang transparan dan akuntabel.*

Penyelenggara jasa internet (disingkat PJI) (bahasa Inggris: *Internet service provider* disingkat *ISP*) adalah perusahaan atau badan yang menyedikan jasa sambungan *internet* dan jasa lainnya yang berhubungan. Kebanyakan perusahaan telepon merupakan penyedia jasa *internet.* Mereka menyediakan jasa seperti hubungan ke *internet,* pendaftaran nama domain dan *hosting*. *ISP* ini mempunyai jaringan baik secara domesik maupun internasional sehingga pelanggan atau pengguna dari sembungan yang disediakan oleh *ISP* dapat terhubung ke jaringan *internet global*. Jaringan sini berupa media transmisi yang dapat mengalirkan data yang dapat berupa kabel (modem, sewa kabel, dan jalur lebar), radio, maupun VSAT.

Nama domain bahasa *inggris* domain *name* adalah nama unik yang diberikan untuk mengidentifikasi nama *server* komputer seperti *web server* di jaringan komputer ataupun *internet.* Nama domain berfungsi untuk

mempermudah pengguna di *internet* pada saat melakukan akses ke *server*, selain juga dipakai untuk mengingat nama *server* yang sikunjungi tanpa harus mengenal deretan angka yang rumit yang dikenal sebagai alamt *IP (Internet Protocol Address* atau sering di singkat *IP*) adalah deretan angka biner atara 32 bit samapi 128 bit yang dipakai sebagai alamat identifikasi untuk komputer *host* dalam jaringan *internet.* Nama domain ini juga dikenal sebagai sebuah kesatuan dari sebuah situs *web* seperti contohnya *"Wikipedia.org".* nama domain kadang-kadang disebut pula dengan istilah *URL,* atau alamat *website.*

Kemarahan publik yang terjadi setelah pemblokiran Vimeo telah menunjukkan bahwa netizen Indonesia semakin lebih sadar akan nilai *Internet* sebagai alat untuk mempromosikan pertumbuhan dan perkembangan, tetapi juga akan hak-hak mereka untuk mengakses, menerima dan menyampaikan informasi dan ide-ide mereka. Kominfo lalu memutar balik anggapan mereka dengan mengatakan bahwa larangan tersebut " tidak permanen, " dan bahwa pemblokiran itu hanya sekedar untuk "menunggu untuk melihat upaya minimum untuk menghapus konten pornografi." Mengingat respon Vimeo bahwa pihaknya "tidak akan mengubah kebijakannya atau menyensor konten apapun dalam menanggapi keputusan Indonesia untuk melarang," maka belum jelas bagaimana situasi ini akan diselesaikan. Kejadian ini menunjukkan bahwa lebih dari sekedar sumber informasi, *Internet* juga memainkan peran penting dalam memfasilitasi partisipasi dan keterlibatan masyarakat, dan karena itu, *Internet* harus tetap terbuka dan dapat diakses.

D. Tata cara Pemblokiran

Prosedur dalam melihat dari peraturan Mentri Komonikasi dan Informatika Republik Indonesia nomer 19 Tahun 2014 tentang penanganan situs internet bermuatan negatif.

Pertama Pelaporan dari Masyarakat Dalam hal Penerimaan laporan berupa pelaporan atas: situs *internet* bermuatan negatif; Pelaporan disampaikan oleh masyarakat kepada Menteri c.q. Direktur Jenderal melalui fasilitas penerimaan pelaporan berupa *e-mail* aduan dan atau pelaporan berbasis situs yang disediakan; Pelaporan dari masyarakat dapat dikategorikan sebagai pelaporan darurat apabila menyangkut hak pribadi, pornografi anak, dan dampak negatif yang cepat di masyarakat dan atau permintaan yang bersifat khusus. Dengan melihat dari Peraturan Menkominfo Nomer 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, pada Bab IV Peran Mayarakat dan Pemerintah, di pasal 10 /11 disebutkan bahwa;

Tata cara penerimaan laporan meliputi:

a. *Penerimaan laporan berupa pelaporan atas:*
    1. *situs internet bermuatan negatif; atau*
    2. *permintaan normalisasi pemblokiran situs.*
b. *Masyarakat menyampaikan laporan kepada Direktur Jenderal melalui fasilitas penerimaan pelaporan berupa e-mail aduan danatau pelaporan berbasis situsyang disediakan;*
c. *Pelaporan dari masyarakat dapat dikategorikan sebagai pelaporan mendesak apabila menyangkut:*

1. *privasi;*
2. *pornografi anak;*
3. *kekerasan;*
4. *suku, agama, ras, dan antargolongan (SARA); dan/atau*
5. *muatan lainnya yang berdampak negatif yang menjadi keresahan masyarakat secara luas.*

Pasal 11

1) *Permintaan pemblokiran sebagaimana dimaksud dalam Pasal 5 ayat (2) harus telah melalui penilaian di kementerian atau lembaga terkait dengan memuat alamat situs, jenis muatan negatif, jenis pelanggaran dan keterangan;*

Laporan harus telah melalui penilaian di Kementerian/Lembaga terkait dengan memuat alamat situs, jenis muatan negatif, jenis pelanggaran dan keterangan; Laporan disampaikan oleh Pejabat berwenang kepada Menteri c.q. Direktur Jenderal, dengan dilampiri daftar alamat situs dan hasil penilaian; Terhadap pelaporan Direktur Jenderal kemudian melakukan pemantauan terhadap situs yang dilaporkan.

Melakukan kegiatan pemberkasan pelaporan yang meliputi: pemberkasan pelaporan asli kedalam berkas dan *database* elektronik berikut penguraian pelaporan; peninjauan ke situs internet yang dituju dan mengambil beberapa sampel situs; dan penampungan sampel gambar situs *internet* ke dalam berkas dan *database* elektronik. Direktur Jenderal menyelesaikan pemberkasan dalam waktu paling lambat 1x24 jam sejak pelaporan diterima; Apabila situs *internet* dimaksud

merupakan situs bermuatan negatif: Direktur Jenderal menempatkan alamat situs tersebut ke dalam *Trust+Positif* dalam periode pemberkasan; apabila merupakan kondisi darurat, Direktur Jenderal menempatkan alamat situs tersebut dalam *Trust+Positif* dalam periode 1x12 jam sejak laporan diterima dan dilakukan komunikasi kepada Penyelenggara Jasa *Akses Internet.*

Kedua Pelaporan dari Kementrian atau Lembaga Pemerintah harus telah melalui penilaian di Kementerian/Lembaga terkait dengan memuat alamat situs, jenis muatan negatif, jenis pelanggaran dan keterangan; Laporan tersebut disampaikan oleh Pejabat berwenang kepada Menteri c.q. Direktur Jenderal, dengan dilampiri daftar alamat situs dan hasil penilaian; Terhadap pelaporan tersebut Direktur Jenderal melakukan pemantauan terhadap situs yang dilaporkan. Tata cara tindak lanjut dan pemberkasan laporan dari Kementerian/Lembaga meliputi: Direktur Jenderal memberikan peringatan melalui *e-mail* kepada penyedia situs untuk menyampaikan adanya muatan negatif. Dalam hal penyedia situs tidak mengindahkan peringatan dalam waktu 2x24 jam, maka dilakukan pemberkasan. Melihat dari Peraturan Menteri Nomer 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, pada Bab IV Peran Mayarakat dan Pemerintah, di pasal 12 disebutkan bahwa;

Kegiatan pengelolaan laporan meliputi:

a. *Penyimpanan laporan asli ke dalam berkas dan database elektronik.*
b. *Peninjauan dan pengambilan sampel ke situs internet yang dituju; dan*
c. *Penyimpanan sampel gambar situs internet ke dalam berkas dan data base elektronik.*

Dalam hal tidak ada alamat komunikasi yang dapat dihubungi maka langsung dilakukan pemberkasan. Melakukan kegiatan pemberkasan pelaporan yang meliputi: pemberkasan pelaporan asli kedalam berkas dan *database* elektronik berikut penguraian pelaporan; peninjauan ke situs *internet* yang dituju dan mengambil beberapa sampel situs; penampungan sampel situs *internet* ke dalam berkas dan *database* elektronik. Direktur Jenderal menyelesaikan pemberkasan dalam waktu paling lambat 5 (lima) hari kerja sejak pelaporan diterima; Apabila situs *internet* dimaksud merupakan situs bermuatan negatif: Direktur Jenderal menempatkan alamat situs tersebut ke dalam *Trust+Positif* dalam periode pemberkasan; apabila merupakan kondisi darurat, Direktur Jenderal menempatkan alamat situs tersebut dalam *Trust+Positif* dalam periode 24 jam sejak laporan diterima dan dilakukan komunikasi kepada Penyelenggara Jasa Akses *Internet*.

Ketiga Pengelola situs atau masyarakat dapat mengajukan normalisasi atas pemblokiran situs. Tata cara pelaporan normalisasi dilakukan sebagaimana dimaksud dalam Pasal 11 Draft. Melakukan kegiatan pemberkasan pelaporan yang meliputi: pemberkasan pelaporan asli kedalam berkas dan data *baseelektronik* berikut penguraian pelaporan; peninjauan ke situs *internet* yang dituju dan mengambil beberapa sampel situs; dan penampungan sampel gambar situs *internet* ke dalam berkas dan data *baseelektronik.*

Direktur Jenderal menyelesaikan pemberkasan dalam waktu paling lambat 1x24 jam sejak pelaporan diterima. Apabila situs *internet* dimaksud bukan merupakan situs bermuatan negatif: menghilangkan dari *Trust+Positif;*

melakukan komunikasi kepada Penyelenggara Jasa Akses *Internet* atas proses normalisasi tersebut; melakukan pemberitahuan (notifikasi) secara elektronik atas hasil penilaian kepada pelapor.

Indonesia adalah negara yang menarik karena tidak adanya standar hukum dan peraturan yang secara sistematis mengatur praktek pengontrolan konten dan kurangnya transparansi dan pengawasan independen atas rezim sensor yang dimandatkan oleh pemerintah, yang mengakibatkan adanya peningkatan risiko pelanggaran hak-hak asasi manusia.

Kementerian Komunikasi dan Informatika (Kominfo) telah dikritik karena mekanisme penyensoran dan penapisan mereka pada umumnya, dan larangan yang ditetapkan baru-baru ini mengenai situs *video-sharing* vimeo pada khususnya. Praktek pemblokiran *domain* seperti *vimeo*, yang dikenal memiliki video-video berkualitas dan berdefinisi tinggi, bisa membahayakan perekonomian dalam jangka panjang karena pasar *e-commerce* di Indonesia berkembang pesat dan adanya peningkatan jumlah usaha yang mempromosikan diri mereka secara *online.* Agar *Internet* dapat terus membantu pertumbuhan ekonomi, kerangka pengontrolan informasi harus konsisten, disederhanakan, dan harmonis agar tidak memberatkan dan lebih transparan dan *accountable*. Sebagai bagian dari pekerjaan kami memantau perkembangan dalam agenda tata kelola *Internet*, laporan ini berusaha untuk menguraikan pengontrolan informasi dan menjelaskan pemblokiran vimeo di Indonesia.