

## **PENYARINGAN KONTEN NEGATIF DI INTERNET**

*memahami konsep dan mengenali kendala implementasinya*

Polemik mengenai perlunya penyaringan konten negatif di internet kembali mengemuka beberapa hari terakhir. Terutama setelah Menteri Komunikasi dan Informatika menyerukan kepada Internet Service Provider (ISP) atau Penyedia Jasa Internet (PJI) untuk melaksanakan kewajiban penyaringan tersebut, yang kali ini disertai dengan penekanan batas waktu hingga satu bulan ke depan.

Namun nampaknya hingga saat ini belum ada kesepakatan dan apalagi titik temu secara teknis pelaksanaan penyaringan yang efektif antara pelaku industri yang dikenai kewajiban dengan Pemerintah yang menginginkan hal ini terwujud segera, mengingat semakin besarnya dampak yang dirasakan oleh masyarakat. Nampaknya kedua belah pihak harus berusaha saling memahami dan membuka peluang kerjasama. Tulisan ini berupaya menjembatani kesenjangan tersebut.

### **Suatu Keniscayaan**

Pada dasarnya penyaringan konten adalah suatu hal yang wajar dan dilakukan oleh hampir semua negara yang memanfaatkan internet. Tujuannya adalah untuk melindungi tatanan sosial masyarakat, norma dan nilai yang diyakini atau dianut oleh negara dan bangsa serta sekaligus menjaga agar iklim industri juga berjalan dalam suasana yang kondusif. Walaupun dengan cara dan sasaran yang berbeda-beda namun sebagian besar penyaringan yang dilakukan oleh negara-negara ini ditujukan kepada konten yang dianggap negatif dan atau melanggar hukum positif yang berlaku di suatu negara. Sehingga penyaringan konten ini dapat dianggap sebagai salah satu upaya menangkal kejahatan di internet.

Sebagai ilustrasi, kebanyakan negara maju di Eropa dan Amerika walaupun permisif terhadap industri konten pornografi namun kenyataannya melakukan pengawasan dan pembatasan akses yang tegas untuk kelompok masyarakat tertentu saja, misalnya berdasarkan umur dan lokasi geografis sesuai dengan budaya setempat. Sedangkan pornografi anak sama sekali dilarang dan selalu dianggap sebagai suatu kejahatan yang amat berat ancamannya.

Di Indonesia, yang dimaksud dengan konten negatif di internet adalah yang mengandung perbuatan yang dilarang di dalam Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu tepatnya pada pasal 27 Ayat 1 (Kesusilaan), Ayat 2 (Perjudian), Pasal 3 (Penghinaan dan atau Pencemaran Nama Baik), Ayat 4 (Pemerasan dan atau Pengancaman) dan Pasal 28 Ayat 1 (Menyebarkan berita bohong), Ayat 2 (SARA). Khusus untuk asusila diambil pula pasal-pasal di dalam Undang Undang Anti Pornografi dan untuk kejahatan terhadap anak-anak digunakan Undang Undang Perlindungan Anak.

### **Kebebasan di Internet**

Namun demikian, ada sebagian kelompok pendukung kebebasan di internet yang khawatir adanya intervensi, apapun itu bentuknya terhadap kehendak masyarakat internet adalah pelanggaran terhadap hak kebebasan berbicara serta berekspresi. Sekalipun itu dilakukan negara berdasarkan hukum positif.

Pada kenyataannya, semua negara demokrasi di dunia mengakui bahwa ada kebebasan berbicara dan berekspresi namun hak ini dibatasi oleh hak orang lainnya. Ketika ada orang lain atau kepentingan publik yang dirugikan, maka kebebasan itu tetap harus dibatasi dan dikendalikan. Dan semua negara yang telah memanfaatkan internet juga telah sepakat bahwa tindak pidana tetapliah suatu perbuatan kriminal, bukan bagian dari kebebasan yang dimaksud di atas.

Sesungguhnya model penyaringan konten internet yang bersifat represif dengan latar belakang ideologi dan politik serta kepentingan nasional hanya terjadi di beberapa (sebagian kecil) negara saja seperti China, Arab Saudi, Iran, Myanmar, Korea Utara, Malaysia dan beberapa negara kecil lainnya yang tidak signifikan jumlahnya. Hal itu biasanya dilakukan dengan cara mengendalikan infrastruktur internet secara keseluruhan untuk membatasi gerakan publik yang menyokong separatisme, keterbukaan dan demokrasi serta HAM yang bertentangan dengan kepentingan kekuasaan dan dianggap mengancam integritas nasional, sekaligus mencegah konten yang dianggap negatif secara universal (asusila, perjudian dll.).

Meskipun demikian, kebijakan pengendalian infrastruktur internet semacam ini juga tidak selalu berkonotasi negatif. Statistik menunjukkan bahwa pada sisi lain kebijakan pengendalian tersebut ternyata dapat meningkatkan kualitas efisiensi akses yang justru memajukan bangsa itu sendiri karena komunitas internetnya lebih fokus di dalam memanfaatkan internet sekaligus menciptakan kemandirian karena negara tersebut tidak lagi tergantung pada layanan internet dan konten dari negara lain. Sehingga potensi dan ekonomi internet lokal pun tumbuh pesat.

### **Konsep Pendekatan**

Pihak Pemerintah, pelaku industri maupun komunitas internet terutama aktivis media alternatif (bloggers/citizen journalism) dan kadangkala kalangan jurnalis media mainstream (terutama online) masih rancu menempatkan penyaringan sebagai suatu sensor. Sesungguhnya konsep pendekatan keduanya berbeda. Di dalam penyaringan, suatu konten negatif telah terlebih dahulu ada/ditayangkan baru kemudian diambil tindakan atau upaya untuk membatasi akses kepadanya sedangkan sensor adalah sebuah proses dimana produksi suatu konten harus mendapatkan persetujuan dari otoritas tertentu sebelum ditayangkan sehingga model sensor adalah pengendalian sepenuhnya terhadap kebebasan berbicara dan berekspresi. Sedangkan penyaringan justru dimaksudkan melindungi dari konten yang tidak dikehendaki oleh publik. Pada prinsipnya sensor mengubah atau menghilangkan sebagian atau seluruhnya suatu konten sedangkan konsep penyaringan hanyalah melakukan penangkalan terhadap konten yang spesifik.

Di Indonesia, polemik terkait konsep kebijakan penyaringan nampaknya terbagi dalam 2 pendapat mainstream. Yang pertama, konsep self filtering (penyaringan sendiri) yang banyak didukung oleh komunitas sipil dan pelaku industri internet selaku pemangku kepentingan. Pendapat pertama ini percaya kepada kearifan para pengguna internet. Untuk mencegah konten negatif dilakukan kampanye berkelanjutan untuk menggugah kesadaran dan memberi keterampilan serta solusi (perangkat, tools, layanan) sehingga para pengguna mampu melindungi dirinya sendiri secara mandiri. Para aktivis, pelaku industri dan pemerintah berperan sesuai kapasitas masing-masing serta bekerjasama menyelenggarakan kegiatan kampanye sebanyak mungkin dan menyebarluaskan solusinya.

Konsep self filtering ini diyakini dapat berjalan efektif apabila didukung oleh semua pelaku yang terlibat di dalam aktivitas berinternet di Indonesia. Secara strategis para aktivis internet percaya bahwa konsep ini dalam jangka panjang lebih mendidik karena turut menyiapkan kesiapan mental pengguna internet. Sekaligus meminimalisir intervensi, arogansi dan penyalahgunaan kewenangan pemerintah di dalam melakukan represi ranah internet dimana hal tersebut dapat berpotensi mencederai hak kebebasan berbicara dan berekspresi.

Yang kedua adalah konsep filtering by design (penyaringan terstruktur) yang banyak didukung oleh para ahli praktisi keamanan internet dan pemerintah. Dalam konsep ini seluruh pemangku kepentingan internet di Indonesia didorong oleh pemerintah untuk bekerja sama membangun suatu layanan penyaringan konten negatif yang terintegrasi dan komprehensif (menyeluruh) diterapkan sesuai dengan tatanan industri internet nasional sebagai suatu tanggung jawab moral bersama. Semua inisiatif diadopsi, difasilitasi dan dilakukan dengan kewenangan (regulasi, birokrasi, represi) pemerintah. Sedang untuk mencegah terjadinya abuse of power (penyalahgunaan) maka sistem yang dibangun harus memungkinkan peran serta masyarakat sipil, komunitas internet dan dunia industri yang lebih dominan dibandingkan dengan pemerintah/kekuasaan.

Konsep filtering by design diyakini dapat berjalan efektif untuk secara instan melindungi para pengguna yang awam, pengguna baru dan anak-anak terutama terhadap praktek penyusutan yang dilakukan oleh penyedia konten negatif. Para pendukung konsep ini percaya bahwa pada prakteknya kemampuan melakukan kampanye kesadaran yang dilakukan oleh pihak manapun sangatlah terbatas dan tidak mampu menjangkau keseluruhan populasi pengguna internet yang terus tumbuh dan berkembang dengan pesat. Sehingga kondisi pada umumnya yang akan terjadi adalah lebih banyak pengguna internet yang tidak terlindungi sehingga ini menimbulkan aneka kerawanan. Maka lebih baik dilakukan proteksi preventif dan reaktif ketimbang menunggu kesadaran dan partisipasi pengguna. Walaupun untuk itu diperlukan effort yang besar serta penataan kembali hingga penyederhanaan tatanan industri internet nasional dan kondisi infrastrukturnya.

Sekedar catatan: dengan tingkat pertumbuhan dan penetrasi internet saat ini, diperkirakan ada 10 ribu pengguna internet baru setiap hari di Indonesia dan lebih dari 40% diantaranya adalah anak-anak remaja usia sekolah menengah.

Sebagian besar bahkan seluruhnya pengguna baru ini adalah sangat awam dan tidak pernah mendapat informasi dan pendampingan untuk melindungi diri dan lingkungan dari dampak negatif internet serta konten negatif yang berbahaya.

## **Pemahaman Teknis**

Para pengambil kebijakan yang nantinya akan membahas penyaringan konten internet pada prinsipnya harus memiliki pemahaman teknis bagaimana internet bekerja dan pada tingkatan mana suatu solusi penyaringan konten akan dapat dilakukan dan model serta teknologi apa saja yang mungkin diterapkan:

1. Penyaringan pada jaringan. Pada prinsipnya internet adalah jaringan global yang menghubungkan titik akses dengan layanan tujuannya. Koneksi internet terjadi sebagai suatu proses dimana perangkat akses akan saling terhubung dengan aneka layanan internet melalui suatu jaringan publik secara terbuka.

Dalam proses ini secara prinsip ada tiga hal yang bekerja yaitu alamat IP (setiap perangkat akses memiliki alamat IP yang unik sebagai pengenalan di dalam jaringan), domain name (sistem pemetaan alamat IP ke nama yang mudah dikenal manusia dan sebaliknya) dan URL (uniform resource locator atau sistem yang mengarahkan pengguna ke suatu lokasi konten tertentu).

Maka teknis penyaringan konten pun dapat dilakukan dengan metode daftar hitam (blacklist) alamat IP, domain dan URL yang dipastikan mengandung konten negatif. Semua ini dapat dilakukan pada tingkat pengguna, tapi untuk hasil yang lebih efektif dan berskala luas harus dilakukan oleh ISP dan NAP.

Karakteristik penyaringan berbasis daftar hitam alamat IP dan domain relatif sifatnya tetap/tidak berubah untuk jangka waktu yang cukup lama sehingga tidak membutuhkan sumber daya yang besar untuk implementasi. Biayanya murah dan mudah direplikasi ke semua ISP karena database blacklist dapat digunakan bersama. Kelemahannya, apabila database daftar hitam semakin besar maka waktu proses (latency) yang diperlukan untuk memeriksa setiap akses yang terjadi mungkin akan meningkat. Namun ada banyak cara untuk mereduksi, misalnya dengan menyediakan active buffer yang lebih besar.

Ada banyak layanan penyedia daftar hitam terkini untuk pemutakhiran data baik yang berbayar (langganan) maupun tidak berbayar. Sehingga setiap ISP dapat leluasa menyelenggarakan penyaringan dengan klasifikasi sesuai selera menyesuaikan dengan kebutuhan pelanggannya. Bahkan mungkin bisa dijual juga sebagai layanan nilai tambah (value added service). Pilihan lain, pemutakhiran dapat melibatkan peran serta komunitas internet secara aktif lewat mekanisme pelaporan dan partisipasi pengklasifikasian konten negatif.

Sedangkan untuk penyaringan URL membutuhkan upaya dan sumber daya yang lebih besar dibandingkan penyaringan berbasis IP dan domain karena suatu URL sifatnya spesifik (langsung mengarah pada lokasi konten tertentu)

dan dinamis (dapat berubah dengan cepat). Penentuan alamat URL berada sepenuhnya dalam kendali pemilik atau penyebar konten tersebut. Sehingga apabila konten tersebut bersifat negatif dan diburu (disaring) oleh banyak pihak maka si pelaku dapat dengan mudah memindahkan lokasinya bahkan menggandakannya di berbagai tempat lain untuk menghindari penangkalan. Bahkan konten ini dapat disisipkan pada konten lain yang sebenarnya baik, sehingga sangat mungkin upaya penyaringan URL yang tidak presisi dapat mengakibatkan turut tersaringnya konten lain yang tidak bersalah. Upaya ini dapat menjadi semakin kompleks apabila pelaku memanfaatkan teknologi penyebaran artifisial secara otomatis sehingga bersifat acak, menyebar luas dan menyamarkan konten tersebut dalam konten-konten biasa lainnya.

Sesuai dengan tatanan industri internet Indonesia saat ini maka sebaiknya proses penyaringan URL dilakukan di tingkat NAP selaku penyelenggara gateway dan exchange bukan di ISP atau apalagi pengguna akhir. Proses ini juga harus melibatkan peran aktif pemerintah sebagai justifikasi penyaringan yang dilakukan. Berbeda dengan penyaringan berbasis IP dan domain yang bisa dilaksanakan secara terbuka melibatkan banyak pihak, maka proses untuk penyaringan URL sebaiknya dilaksanakan secara tertutup, cermat, berhati-hati serta melibatkan segelintir pihak yang tidak hanya kompeten tetapi juga memiliki kewenangan sesuai peraturan perundangan yang ada.

Penyaringan berbasis IP, domain dan URL adalah jenis filtering by design.

2. Penyaringan pada aplikasi. Pada dasarnya konten negatif sebenarnya dapat menyebar dengan berbagai macam cara memanfaatkan keawaman pengguna dan kelemahan aplikasi yang digunakannya. Sehingga konsep self filtering dimaksudkan untuk mengatasi permasalahan ini. Intinya pengguna diajak meningkatkan kesadaran dan keterampilannya agar mampu melindungi diri dan turut serta menangkal penyebaran konten negatif di lingkungannya.

Ada banyak solusi untuk melakukan proteksi dan penyaringan aplikasi yang digunakan untuk akses internet. Misalnya menggunakan teknik deteksi kata kunci (keyword), pengenalan artifisial (regex) dan daftar putih (whitelist). Semua ini dikombinasikan pula dengan sistem dan teknologi anti virus, anti malware dan personal firewall yang terintegrasi di dalam sistem operasi.

Sistem perlindungan pengguna pada umumnya sudah tersedia secara default di setiap aplikasi, akan tetapi perlu diaktifkan/dikonfigurasi secara manual. Apabila aplikasi yang digunakan seperti email agent, web browser belum menyediakan fasilitas ini maka pengguna dapat memasang produk pihak ketiga baik yang berbayar maupun yang tidak berbayar. Banyak pilihannya.

Walaupun pada dasarnya penyaringan pada aplikasi dapat dilakukan sendiri oleh pengguna akan tetapi ISP sudah seharusnya juga menyediakan layanan dukungan teknis sekaligus menyediakan aneka pilihan aplikasi perlindungan beserta pemutakhirannya apabila sekiranya nanti pengguna membutuhkan.

## Tantangan Implementasi

Secara teoritis dan teknis penyaringan konten negatif sangat mungkin dilakukan baik di tingkat jaringan melibatkan penyelenggara (NAP dan ISP) maupun pada tingkat pengguna (self filtering). Tetapi ada beberapa hal yang patut dicermati berdasarkan pengalaman implementasi penyaringan konten negatif di negara lain dan inisiatif yang dilakukan oleh komunitas internet Indonesia selama ini.

1. Masalah volume. Pertumbuhan konten termasuk yang negatif, pengguna dan traffic internet itu sendiri sangat pesat dan eksponensial. Sehingga upaya penyaringan akan membutuhkan upaya dan sumber daya serta biaya yang semakin meningkat. Maka sebelum kebijakan penyaringan diterapkan, terlebih dahulu harus ada konsep dan desain serta rencana implementasi komprehensif serta telah teruji (proven) kehandalannya untuk menangani skala yang luas dan terus tumbuh. Pemerintah dan industri yang terlibat harus mampu menjamin aspek keberlangsungannya, karena sistem itu akan dibutuhkan jangka panjang.
2. Masalah kejenuhan. Bagaimanapun sistem penyaringan ini masih akan membutuhkan intervensi manual terutama untuk dua hal melakukan klasifikasi jenis konten negatif apakah itu tergolong sebagai pornografi, judi dll. dan untuk melakukan pemeriksaan apakah konten yang dilaporkan masyarakat memang benar mengandung unsur negatif yang dilarang sekaligus melakukan pengujian apakah penyaringan yang dilakukan telah tepat sasaran. Pengalaman inisiatif sistem DNS filtering Nawala Project yang diselenggarakan oleh Asosiasi Warung Internet Indonesia (AWARI) dalam sehari bisa diterima 200 lebih email pengaduan. Pemeriksaan dan klasifikasi adalah pekerjaan yang melelahkan dan mengakibatkan kejenuhan mental dan pikiran yang luar biasa serta diperlukan kemampuan ketahanan tersendiri untuk melakukannya. Apalagi bila proses itu dikerjakan oleh relawan (voluntary), maka akan sangat sulit dijamin kecepatan respon pengaduan dan akurasi proses pemutakhiran data daftar hitam. Sangat mungkin terjadi kesalahan akibat kekurangcermatan dan kelelahan mental. Maka harus dipikirkan kesiapan sumber daya manusia dari segi jumlah serta jadwal rotasi yang wajar untuk mengantisipasi pertumbuhan pengaduan konten.
3. Masalah justifikasi. Suatu konten sebelum diklasifikasi dan dimasukkan ke dalam daftar hitam penyaringan harus mendapatkan justifikasi sebab musabab mengapa konten tersebut dianggap mengandung unsur negatif. Pemerintah harus menghimpun sekelompok orang yang dianggap mewakili kepentingan dan sudut pandang yang ada di dalam masyarakat untuk melakukan justifikasi. Kelemahannya, belum tentu justifikasi itu diterima oleh kelompok lain atau minoritas yang terabaikan. Hal semacam ini justru bisa menjadi preseden praktek demokrasi yang buruk. Kesalahan dan bias subyektif di dalam justifikasi bisa jadi berakibat fatal, sebagai contoh

pengalaman yang terjadi di Nawala Project. Penyaringan terhadap suatu situs yang memuat konten perdebatan agama yang cenderung mengarah kepada unsur SARA justru mendapatkan pertentangan dari kelompok yang merasa dihilangkan hak jawabnya oleh sistem penyaringan karena mereka tidak lagi leluasa mengakses situs debat tersebut. Apalagi sebenarnya di dalam pemahaman dan definisi konten negatif menurut undang-undang pun ternyata masih menyisakan ruang interpretasi yang berbeda.

4. Masalah kebutuhan khusus. Dalam banyak aspek suatu sistem penyaringan sangat mungkin menghambat kegiatan tertentu yang sangat penting dan strategis seperti penelitian/riset, intelejen/data mining, sistem deteksi dini terhadap anomali infrastruktur internet hingga proses penegakan hukum. Sebagai ilustrasi: upaya pelacakan dan pengumpulan alat bukti serta petunjuk di dalam proses penyelidikan dan penyidikan kasus penyebaran konten negatif justru memerlukan akses yang bebas terhadap material tersebut. Untuk keperluan penyediaan alat bukti digital forensic (digital evidence containment) bahkan harus dilakukan retensi bukan hanya oleh penegak hukum tetapi juga pihak penyelenggara (misalnya web hosting atau content provider). Prosedur ini sangat diperlukan di dalam rekonstruksi pengungkapan tindak kejahatan digital. Apabila tekanan ketentuan penyaringan kurang memperhitungkan kebutuhan penegakan hukum, kebijakan tersebut justru akan mendorong penyelenggara untuk melakukan tindakan yang justru mengakibatkan hilangnya alat bukti, menghapus jejak pelaku dan menyulitkan proses hukum di kemudian hari.
5. Masalah peralihan saluran penyebaran. Pengendalian konten harus dilakukan secara cermat, hati-hati, memperhatikan momentum di masyarakat serta tidak terburu-buru. Kearifan diperlukan justru untuk menjamin keberhasilan upaya ini dalam jangka panjang. Sebab di dalam proses penyaringan sebenarnya berlaku hukum balon, yaitu apabila dipencet hingga mengempis pada satu sisi justru akan mengembang luas di sisi yang lain. Penyaringan konten negatif pada layanan yang berada di saluran terbuka justru akan mendorong penyebaran melalui saluran yang tertutup dan lebih bersifat pribadi (private). Misalnya, penyaringan situs pornografi mungkin akan mendorong penyebaran konten negatif ini melalui saluran email, peer to peer file sharing dlsb. dimana akses yang bersifat tertutup dan pribadi (private) seperti ini tentu saja sangat sulit untuk ditangkal dan sudah masuk ke wilayah hak individu yang justru harus dilindungi sesuai prinsip Hak Asasi Manusia.
6. Perkembangan akses seluler. Semua pihak kini mengkritisi penyebaran konten negatif pada saluran internet konvensional dan menyatakannya sebagai situasi yang kritis. Namun sebenarnya ada saluran lain yang luput dari perhatian kita yaitu akses seluler. Apabila kita memperhatikan angka statistiknya maka segera dapat disadari bahwa masa depan internet justru ada di saluran seluler ini. Dalam 15+ tahun usia internet konvensional Indonesia hanya mampu menghimpun 45 juta pengguna. Sementara akses

data internet melalui jalur selular berhasil mencapai angka penetrasi 45 juta hanya dalam waktu 5 tahun. Dari segi perangkat akses, internet konvensional saat ini hanya memiliki sekitar 8+ juta terminal (komputer) sementara untuk akses selular ada 85 juta perangkat yang sudah GPRS/EDGE, UMTS/HSDPA (3G), EVDO ready. Model bisnis layanan selular sangatlah berbeda dengan layanan internet biasa, dimana pemilik dan pelanggan selular tidak serta merta menjadi pengguna akses data/internet. Sehingga cara pendekatan dan edukasi penggunaannya pun berbeda namun ironisnya justru Pemerintah selaku regulator yang hendak mendorong implementasi penyaringan konten negatif sama sekali belum mengajak dan atau mewajibkan para operator selular sebagaimana dikenakan pada ISP dan NAP.

7. Penyebaran offline. Bahwa antara dunia nyata dan dunia maya pada saat ini bukanlah dua ranah yang terpisah namun justru saling terkait erat satu sama lain. Yang terjadi di ranah internet juga membawa dampak ke ranah nyata dan sebaliknya. Sehingga dalam kaitan upaya penyaringan konten negatif di internet harus pula diiringi dengan gerakan yang serupa di ranah nyata ini dan dilaksanakan secara bersamaan, intensif serta berkelanjutan. Apabila tindakan dan sikap tegas tidak dilakukan di kedua ranah maka niscaya akan terjadi efek ping pong dimana konten negatif akan berpindah-pindah dari ranah maya ke ranah nyata dan sebaliknya.

Demikianlah, kiranya tulisan ini dapat mengawali wacana untuk menuju suatu kesepahaman dan kesamaan persepsi antara seluruh pemangku kepentingan yang terlibat di dalam inisiatif ini. Semoga internet Indonesia semakin maju, aman dan nyaman terbebas dari gangguan konten negatif dan berganti dengan tumbuhnya konten positif yang bermanfaat, memajukan dan mensejahterakan.

*(M. Salahuddien, penulis adalah aktivis, praktisi dan konsultan Teknologi Informasi, saat ini menjabat sebagai Wakil Ketua ID-SIRTII yaitu Indonesia Security Incident Response Team On Internet Infrastructure)*