

Merumuskan kebijakan penata-kelolaan internet berbasis hak¹

Oleh: Wahyudi Djafar²

“internet tidaklah dibangun sebagai sebuah ‘zona bebas hukum’, pengaturan tetap dibolehkan khususnya dalam rangka melindungi konsumen dan anak-anak.”³

Akses internet sebagai hak asasi manusia

Navi Pillay, Komisioner Tinggi HAM PBB, menyatakan bahwa internet merupakan tren global yang paling kuat, yang telah menghadirkan suatu tantangan HAM sangat kompleks. Internet telah menghapuskan berbagai upaya untuk membentuk monopoli informasi dan berita, sehingga mampu mendorong beragam pengambilan keputusan pemerintah secara transparan dan akuntabel.⁴ Memang, besarnya pengguna internet di dunia telah melahirkan banyak peluang. Mencuplik pernyataan Frank La Rue, Pelapor Khusus PBB untuk Kebebasan Berpendapat dan Berekspresi, internet telah menjadi alat yang sangat diperlukan untuk mewujudkan berbagai hak asasi manusia, memberantas ketidakadilan, dan mempercepat pembangunan dan kemajuan manusia. Oleh karena itu, memastikan akses universal terhadap internet harus menjadi prioritas semua negara.⁵

Dalam konteks itu pula, Dewan HAM PBB telah mengeluarkan Resolusi A/HRC/20/L.13 tentang *The promotion, protection and enjoyment of human rights on the Internet*, pada 29 Juni 2012. Dalam resolusi tersebut, Dewan HAM menegaskan antara lain: setiap orang memiliki perlindungan hak yang sama baik offline maupun online, sebagaimana dijamin oleh Kovenan Internasional Hak-hak Sipil dan Politik, serta Deklarasi Umum Hak Asasi Manusia; sifat global dan terbuka dari internet diakui sebagai kekuatan pendorong dalam mempercepat kemajuan pembangunan dalam berbagai bentuk; meminta kepada seluruh negara untuk mempromosikan dan memfasilitasi akses ke Internet dan kerjasama internasional yang bertujuan untuk pengembangan media, informasi dan fasilitas komunikasi di semua negara.⁶ Dalam konteks itulah kebijakan penata-kelolaan internet di bangun oleh semua negara. Hak asasi manusia menjadi instrumen paling kunci di dalam mempersiapkan rumusan setiap kebijakan yang terkait dengan pemanfaatan dan pengembangan internet.

Problem dalam pengaturan konten

Di Indonesia, pengaturan mengenai konten internet pertama kali mengemuka di dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun demikian ketentuan mengenai konten internet di dalam UU ITE lebih menekankan pada pengaturan mengenai konten-konten yang dilarang atau masuk kategori kejahatan jika dilakukan. Ketentuan tersebut seperti diatur dalam Pasal 27, Pasal 28 dan Pasal 29 UU ITE. Konten-konten internet

¹ Bahan Internet Briefing dan Diskusi Publik: Mengawal Kebijakan Internet Indonesia Paska Pertemuan IGF 2013, Jakarta, 4 Desember 2013.

² Peneliti dan Pengacara Publik pada Lembaga Studi dan Advokasi Masyarakat (ELSAM).

³ Laporan Pelapor Khusus PBB untuk Kebebasan Berpendapat dan Berekspresi, Abid Husain, tahun 1999 (E/CN.4/1999/64), dapat diakses di <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G99/107/66/PDF/G9910766.pdf?OpenElement>.

⁴ Lihat Navi Pillay, Human Rights Achievements and Challenges in a Rapidly Changing World, pidato di University of Witwatersand, Johannesburg, 17 April 2013, dapat diakses di <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13250&LangID=E>.

⁵ Lihat Laporan Frank La Rue Paragraf 59, A/HRC/14/23, dapat diakses di <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf>.

⁶ Lihat A/HRC/20/L.13, dapat diakses di <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

yang dilarang menurut ketentuan tersebut meliputi: (i) konten yang dianggap melanggar kesusilaan; (ii) konten yang mengandung muatan perjudian; (iii) konten yang memuat unsur penghinaan dan/atau pencemaran nama baik; (iv) konten yang mengandung unsur pemerasan dan/atau pengancaman; (v) konten yang menyebarkan berita bohong sehingga menimbulkan kerugian konsumen; (vi) konten yang menimbulkan kebencian berdasar SARA; dan (vii) konten yang mengandung muatan ancaman kekerasan.

Selain ketentuan di dalam UU ITE, ketentuan yang mengatur konten internet juga ditemukan di dalam Pasal 18 huruf a UU No. 44 Tahun 2008 tentang Pornografi. Pada ketentuan tersebut dikatakan, bahwa untuk mencegah perluasan pornografi, pemerintah dapat melakukan pemutusan jaringan pembuatan dan penyebarluasan produk pornografi atau jasa pornografi, termasuk pemblokiran pornografi melalui internet. Secara umum, mengacu pada Pasal 40 ayat (2) UU ITE, tindakan pembatasan dan pengawasan terhadap konten internet di Indonesia dilakukan pemerintah dalam rangka melindungi kepentingan umum dari segala jenis gangguan penyalahgunaan informasi dan transaksi elektronik yang mengganggu ketertiban umum.

Masalahnya, meski UU ITE telah mengidentifikasi konten-konten yang dilarang, namun undang-undang ini belum menyediakan pengaturan yang memadai pengawasan dan mekanisme pembatasan terhadap konten-konten tersebut, termasuk tata cara (hukum acara) di dalam melakukan penyaringan dan pemblokiran konten. Merujuk pada laporan yang disusun oleh Pelapor Khusus PBB untuk kebebasan berekspresi dan berpendapat, disebutkan bahwa pemblokiran adalah tindakan-tindakan yang dilakukan untuk mencegah konten tertentu mencapai pengguna akhir. Hal tersebut meliputi pencegahan pengguna dalam mengakses laman khusus, Internet Protocol (IP), alamat, ekstensi nama domain, penutupan laman dari laman server di mana mereka menempatinya, atau menggunakan teknologi filter untuk membuang halaman-halaman yang mengandung kata kunci tertentu atau memblok konten tertentu agar tidak bisa muncul.⁷

Selain tindakan-tindakan yang masuk dalam cakupan di atas, baru-baru ini juga muncul tren pemblokiran berdasarkan waktu (*just-in-time*), yang dilakukan untuk mencegah pengguna agar tidak mengakses atau menyebarkan informasi dengan kata kunci tertentu dalam waktu tertentu. Hal ini misalnya dalam momen-momen politik, seperti pemilihan umum, konflik sosial, atau peringatan kejadian bersejarah atau politik yang bermakna. Selama kurun waktu tersebut, laman milik pihak-pihak oposisi, media independen, dan aplikasi jaringan sosial seperti Twitter dan Facebook dilakukan pemblokiran, seperti yang dapat disaksikan dalam peristiwa demonstrasi yang terjadi di wilayah Timur Tengah dan Afrika Utara.⁸

Dalam banyak kasus, pembatasan, pengawasan, manipulasi dan sensor konten internet telah dilakukan oleh negara tanpa dasar hukum, atau meski berdasarkan hukum, namun aturannya terlalu luas dan ambigu. Selain itu tindakan tersebut juga seringkali dilakukan tanpa adanya pembenaran tujuan atau dengan cara yang jelas-jelas tidak perlu dan/atau tidak seimbang dalam mencapai tujuan. Tindakan sensor terhadap konten internet, dalam bentuk pemblokiran dan penapisan dengan menggunakan teknologi tertentu adalah suatu tindakan pelanggaran terhadap hak atas kebebasan berekspresi. Tindakan-tindakan tersebut benar-benar tidak sesuai dengan kewajiban negara di bawah hukum hak asasi manusia, dan sering menciptakan “chilling effect” atau efek ketakutan yang besar terhadap kebebasan berpendapat dan berekspresi.

⁷ Lihat A/HRC/17/27, paragraf 29, dapat diakses di http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Dalam laporannya Frank La Rue menyontohkan China sebagai salah satu negara yang mempunyai sistem penyaringan paling luas dan sangat bagus dalam mengontrol informasi di Internet. China telah mengadopsi sistem filter yang luas dalam mengblokir akses ke laman-laman yang mempunyai kata kunci tertentu misalnya “democracy” dan “human rights”.

⁸ Lihat Ibid., paragraf 30.

Mengacu pada laporan Frank La Rue, tindakan pemblokiran dan penapisan konten internet masuk dalam kategori pelanggaran, jika tindakan dilakukan dalam situasi berikut ini: *Pertama*, kondisi khusus yang membenarkan pemblokiran tidak terdapat dalam hukum, atau diatur oleh hukum namun pengaturannya sangat luas dan tidak langsung, sehingga menyebabkan pemblokiran konten secara luas dan semena-mena; *Kedua*, pemblokiran tidak dilakukan untuk memenuhi tujuan yang dijelaskan Pasal 19 ayat (3) ICCPR, dan daftar pemblokiran secara umum dirahasiakan sehingga sulit untuk ditentukan apakah akses ke konten yang dibatasi tersebut dilakukan demi tujuan yang benar; *Ketiga*, bahkan ketika pembenaran terhadap pemblokiran dilakukan, tindakan pemblokiran telah menciptakan alat-alat yang tidak perlu dan tidak sesuai untuk mencapai tujuan karena tindakan tersebut sering tidak mempunyai tujuan yang cukup untuk dilakukan dan menyebabkan konten tidak bisa diakses karena dianggap ilegal; dan *Keempat*, pemblokiran dan penapisan dilakukan tanpa adanya intervensi atau kemungkinan pengujian kembali oleh sebuah pengadilan atau badan independen.⁹

Sebagaimana halnya penemuan teknologi teknologi lainnya, teknologi internet juga bisa disalahgunakan yang dapat menyebabkan kerugian bagi pihak lain. Oleh karena itu pembatasan terhadap konten internet juga mungkin dilakukan, khususnya terhadap jenis-jenis berikut ini: (i) informasi yang mengandung muatan pornografi anak (untuk menjaga hak-hak anak),¹⁰ (ii) penyebaran kebencian (untuk melindungi hak-hak komunitas yang terpengaruh oleh hal itu),¹¹ (iii) pencemaran nama baik (untuk menjaga hak dan reputasi orang lain dari serangan pihak-pihak yang tidak bertanggungjawab), hasutan publik untuk melakukan genosida (untuk melindungi hak-hak orang lain),¹² dan (iv) advokasi nasional, ras atau agama yang bisa memicu hasutan diskriminasi, kekerasan atau permusuhan (untuk menjaga hak-hak orang lain, seperti hak untuk hidup).¹³

Namun demikian, ketika pembatasan diberlakukan terhadap konten internet sebagai tindakan pengecualian pada konten dalam jaringan, pembatasan tersebut harus melalui tiga bagian pengujian yang sifatnya kumulatif: (1) pembatasan tersebut harus diatur oleh hukum, yang jelas dan dapat diakses oleh semua orang (prinsip-prinsip prediktabilitas dan transparansi); (2) pembatasan tersebut harus memenuhi salah satu tujuan yang diatur pada Pasal 19 ayat (3) ICCPR, yaitu (i) untuk melindungi hak-hak dan reputasi orang lain; (ii) untuk melindungi keamanan nasional atau ketertiban umum, atau kesehatan atau moral publik (prinsip legitimasi); dan (3) pembatasan itu harus dapat dibuktikan bahwa penting dilakukan dan cara-cara pembatasan seminimal mungkin diperlukan untuk mencapai tujuan utama (prinsip-prinsip kepentingan dan keberimbangan/proporsionalitas). Lebih lanjut, legislasi apapun yang membatasi hak atas kebebasan berekspresi harus diaplikasikan oleh badan yang independen dari pengaruh politik, komersial atau pihak yang tidak berwenang, tidak secara semena-mena ataupun diskriminatif. Harus ada perlindungan untuk menghadapi penyalahgunaan termasuk kemungkinan terhadap tantangan dan pemulihan atas penerapan pembatasan yang disalahgunakan.

Privasi: masalah aktual yang memerlukan penanganan cepat

Praktik intervensi terhadap privasi, dalam bentuk *surveillance*, intersepsi komunikasi dan gangguan terhadap data pribadi menjadi salah satu persoalan besar yang mengemuka dalam pemanfaatan teknologi informasi dan komunikasi khususnya internet. Pelapor khusus PBB

⁹ Lihat *Ibid.*, paragraf 31.

¹⁰ Penyebaran pornografi anak dilarang oleh hukum hak asasi manusia internasional, lihat *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, art. 3, para. 1 (c).

¹¹ Lihat contoh *Faurisson v. France*, Komite Hak Asasi Manusia PBB, Resolusi 550/1993, pandangan-pandangan pada tanggal 8 November 1996. Isu mengenai pernyataan kebencian juga telah dijelaskan pada laporan sebelumnya, lihat antara lain E/CN.4/1999/63; E/CN.4/2000/63; E/CN.4/2002/75; dan A/HRC/4/27.

¹² Lihat contoh Pasal 3 (c) Konvensi Pencegahan dan Penghukuman Kejahatan Genosida.

¹³ Lihat contoh Pasal 20 ayat (2) Kovenan Internasional Hak-hak Sipil dan Politik.

untuk kebebasan berpendapat dan berekspresi Frank La Rue, telah memberikan perhatian khusus terhadap soal ini, mengingat tingginya praktik pengamatan (*surveillance*), intersepsi komunikasi pribadi warga negara, serta pemindahtanganan data pribadi secara sewenang-wenang. Dalam laporannya, La Rue menegaskan perlunya setiap negara memiliki undang-undang yang secara jelas menggambarkan kondisi-kondisi bahwa hak atas privasi dari individu bisa dibatasi di bawah kondisi-kondisi tertentu, dan tindakan-tindakan menyentuh hak ini harus diambil dengan dasar sebuah keputusan khusus. Keputusan ini diambil oleh otoritas negara yang dijamin secara jelas oleh hukum untuk melakukan tindakan tersebut.¹⁴

Baru-baru ini, Selasa 26 November 2013, menyikapi terbongkarnya praktik-praktik *surveillance* dan penyadapan yang dilakukan oleh sejumlah negara, terutama Amerika Serikat, melalui National Security Agency, Dewan HAM PBB telah mengeluarkan sebuah resolusi tentang hak atas privasi di era digital. Melalui resolusi tersebut, Dewan HAM mengingatkan kepada seluruh negara untuk melindungi dan menghormati hak atas privasi, sebagaimana dijamin Pasal 17 Kovenan Hak-hak Sipil dan Politik, serta Pasal 12 Deklarasi Umum Hak Asasi Manusia. Selain itu Dewan HAM juga meminta kepada negara-negara melakukan peninjauan kembali prosedur mereka, terutama peraturan perundang-undangan yang mengatur mengenai *surveillance*, intersepsi dan pengumpulan data pribadi, dengan tujuan untuk menegakkan hak atas privasi serta memastikan pelaksanaan penuh dan efektif semua kewajiban di bawah hukum hak asasi manusia internasional.¹⁵

Secara sederhana hak atas privasi didefinisikan sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. Keluasan cakupan privasi bisanya menjadikan banyaknya pengaturan mengenai privasi di suatu negara, baik dalam jenis maupun tingkatnya.¹⁶ Di Indonesia sendiri, pasca-amandemen konstitusi, hak atas privasi diakui sebagai salah satu hak konstitusional warga negara yang harus dilindungi. Perlindungan ini ditegaskan di dalam Pasal 28 G ayat (1) UUD 1945, yang diantaranya menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi (privasi), keluarga, kehormatan, martabat, dan harta bendanya (termasuk data-data pribadi). Pernyataan tersebut juga ditegaskan di dalam Pasal 32 UU No. 39 Tahun 1999 tentang HAM, yang antara lain menyatakan bahwa kemerdekaan dan rahasia komunikasi melalui sarana elektronik tidak boleh diganggu kecuali atas perintah hakim atau kekuasaan lain yang sah menurut undang-undang.

Intersepsi komunikasi secara melawan hukum yang dilakukan di internet juga dilarang menurut hukum Indonesia. Larangan ini ditegaskan di dalam Pasal 31 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.¹⁷ Dalam ketentuan tersebut dinyatakan bahwa setiap orang dilarang untuk melakukan intersepsi atau penyadapan atas informasi atau dokumen elektronik dalam suatu komputer atau sistem elektronik milik orang lain. Intersepsi komunikasi hanya dibolehkan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan atau institusi penegak hukum lainnya. Pelanggaran terhadap ketentuan tersebut diancam pidana penjara selama-lamanya 10 tahun dan/atau denda sebanyak-banyaknya 800 juta rupiah.¹⁸

Namun demikian ketiadaan aturan tunggal tentang tata cara penyadapan di Indonesia telah menciptakan kerentanan terhadap tindakan intersepsi komunikasi pribadi warga negara,

¹⁴ Lihat Laporan Frank La Rue Paragraf 59, A/HRC/14/23, dapat diakses di <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf>.

¹⁵ Lihat http://www.auswaertiges-amt.de/cae/servlet/contentblob/660692/publicationFile/186838/131127_Right2Privacy_EN.pdf.

¹⁶ Lihat A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), hal. 7-8.

¹⁷ Larangan serupa juga diatur di dalam Bab XXVIII KUHP tentang Kejahatan Jabatan terutama di dalam Pasal 430 sampai dengan 434. Khusus mengenai larangan penyadapan terhadap komunikasi jarak jauh melalui alat, diatur di dalam Pasal 433, yang melarang penyadapan telepon dan telegraf secara ilegal. Juga dapat kita temukan di dalam Pasal 40 UU No. 36 Tahun 1999 tentang Telekomunikasi.

¹⁸ Lihat Pasal 31 ayat (2) jo. Pasal 47 UU ITE.

termasuk komunikasi menggunakan internet, seperti surat elektronik serta bermacam perangkat media sosial. Sampai hari ini, Indonesia sedikitnya memiliki dua belas peraturan perundang-undangan yang di dalamnya mengatur tentang penyadapan/intersepsi komunikasi dengan tata cara yang berbeda-beda. Perbedaan pengaturan mengenai penyadapan ini misalnya nampak sangat nyata antara UU Pemberantasan Tindak Pidana Terorisme, UU Narkotika, UU Komisi Pemberantasan Tindak Pidana Korupsi, dan UU Intelijen Negara. Centang-perenangannya hukum penyadapan di Indonesia ini telah membuka celah yang lebar bagi praktik campur tangan terhadap komunikasi pribadi warga negara, termasuk yang menggunakan internet.¹⁹

Selain masalah centang-perenang hukum penyadapan, problem lain yang mengemuka dalam perlindungan privasi di Indonesia adalah tidak memadainya perlindungan terhadap data pribadi warga negara. Bahkan sampai saat ini, Indonesia belum memiliki peraturan perundang-undangan yang secara khusus menjamin perlindungan data pribadi seseorang. Ketentuan mengenai perlindungan data pribadi seseorang, khususnya yang dalam bentuk elektronik diatur secara terbatas di dalam Pasal 26 dan Pasal 43 ayat (2) UU Informasi dan Transaksi Elektronik. Namun pelanggaran terhadap ketentuan ini tidak diancam dengan pidana, hanya diberikan ruang untuk melakukan ganti kerugian.²⁰ Lemahnya pengaturan mengenai perlindungan data pribadi berakibat pada maraknya praktik pembocoran dan pemindatanganan data pribadi seseorang di Indonesia, khususnya untuk kepentingan komersial.²¹

Penatakelolaan dengan multi-pemangku kepentingan

Berbicara mengenai tata kelola internet adalah mendiskusikan suatu topik yang besar, kompleks, sekaligus ambigu.²² Pengalaman di beberapa negara, seperti Filipina, Brazil dan Yordania, memperlihatkan bahwa model pembentukan regulasi yang bersifat dari atas (*top down*) dalam sektor internet, hanya akan melahirkan suatu aturan yang represif dan menimbulkan risiko bagi publik. Oleh karena itu yang paling tepat adalah menciptakan aturan sektor internet dengan melibatkan banyak pemangku kepentingan, sehingga bisa tercipta suatu aturan yang menjunjung tinggi kebebasan berinternet, tetapi pada sisi lain juga mampu meminimalisir dampak negatif dari penggunaan teknologi ini. Tegasnya, skema multi-pihak penting dijalankan dalam pembentukan regulasi yang terkait dengan internet, mengingat besarnya pihak yang terlibat dalam pemanfaatan teknologi ini, juga dampak yang ditimbulkan. []

¹⁹ Lihat Wahyudi Djafar, Protecting privacy rights from wiretapping, The Jakarta Post, 21 Februari 2013, dapat diakses di <http://www.thejakartapost.com/news/2013/02/21/protecting-privacy-rights-wiretapping.html>. Lihat Laporan Pelapor Khusus PBB untuk kebebasan berekspresi dan berpendapat, Frank La Rue, A/HRC/23/40, dapat diakses di http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

²⁰ Lihat Pasal 26 ayat (2) UU ITE. Lebih jauh pemerintah telah mengeluarkan PP 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

²¹ Lihat Wahyudi Djafar, Kita Perlu UU Perlindungan Data Pribadi, dalam <http://www.hukumpedia.com/ham/kita-perlu-uu-perlindungan-data-pribadi-hk51da54d24bb82.html>.

²² Lihat Lawrence B. Solum, Models of Internet Governance, dalam Lee A. Bygrave and Jon Bing, *Internet Governance Infrastructure and Institutions*, (Oxford: Oxford University Press, 2009), hal. 48.