

Position Paper

RUU KEAMANAN DAN KETAHANAN SIBER: PROBLEM DALAM PENGATURAN DAN ANCAMANNYA TERHADAP KEBEBASAN SIPIL



2019

A. PENGANTAR

Pada Juli 2019 yang lalu, Dewan Perwakilan Rakyat (DPR) telah menetapkan Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber menjadi usul inisiatif DPR, untuk dilakukan pembahasan bersama dengan pemerintah. Dalam internal pemerintah sendiri saat ini tengah mencoba untuk merampungkan proses penyusunan Daftar Inventaris Masalah (DIM) RUU tersebut, sebagai syarat untuk dilakukan pembahasan.

Melihat proses yang berkembang, nampak ada upaya dari sejumlah pihak untuk mempercepat proses pembahasan RUU ini, dan mengesahkannya sebelum berakhirnya periode DPR 2014-2019. Padahal mencermati materinya, RUU ini belum dapat dikatakan sebagai aturan keamanan siber yang baik, mengingat adanya sejumlah inkonsistensi pengaturan antar-pasal, ketidakjelasan fokus pengaturan, hingga besarnya potensi ancaman terhadap kebebasan sipil.

Secara umum, pembahasan RUU Keamanan dan Ketahanan Siber cenderung dilakukan secara tergesa gesa dan minim partisipasi publik. Kondisi ini menimbulkan dugaan kecurigaan adanya kepentingan di balik pembahasan RUU ini. Padahal prinsip utama dalam pembuatan perundang undangan itu harus dilakukan secara transparan dan melibatkan partisipasi publik yang luas.

Sebagai sebuah rancangan aturan yang akan menjadi panduan dalam keamanan siber di Indonesia, rumusan RUU ini sangat menekankan pada pendekatan *"state centric"*, sehingga gagal untuk memberikan kejelasan untuk memastikan perlindungan keamanan individu, perangkat, dan jaringan dalam ruang siber.

Selain itu, pada ketentuan umumnya, RUU ini juga lebih banyak memberikan definisi yang identik dengan pengaturan keamanan nasional pada aspek pertahanan, tetapi malah melupakan elemen-elemen dalam keamanan siber, seperti sistem komputer, perangkat, jaringan siber.

Perumusan aturan dalam rancangan ini juga telah menciptakan ambiguitas dalam tata kelola dan kerangka kerja kelembagaan yang berwenang dalam pengelolaan keamanan siber, yang berpotensi overlapping kewenangan, bahkan sengketa kewenangan diantara mereka. RUU ini belum mampu mengidentifikasi dengan baik kebutuhan kebijakan dan peran bagi tiap sektor dalam penyelenggaraan keamanan siber, sehingga belum bisa menghadirkan kerangka kerja dan tata kelola keamanan siber yang baik dan jelas. Situasi ini justru dapat menciptakan kerentanan dan kerawanan dalam keamanan siber, khususnya bagi bisnis dan masyarakat sebagai pengguna, karena adanya ketidakpastian dalam pembagian peran antar-sektor.

Dalam menghadapi ancaman siber, pemerintah sudah memiliki beragam aturan dan institusi yang berkerja untuk menanganinya sesuai dengan fungsi dan tugasnya masing masing. Dengan demikian, tidak cukup alasan untuk DPR tergesa-gesa membahas RUU ini. Jikapun terjadi serangan siber maka institusi yang ada sudah bisa digunakan untuk menangani insiden tersebut.

Lebih lanjut, meski dalam salah satu pasalnya dikatakan dalam penyelenggaraan keamanan dan ketahanan siber harus selalu mengedepankan penghormatan terhadap hak asasi manusia, namun jika membaca keseluruhan rumusannya, justru kental nuansa pembatasan terhadap kebebasan sipil. Hal ini salah satunya nampak dari pemberian wewenang yang sangat besar bagi BSSN untuk melakukan tindakan penapisan konten dan aplikasi elektronik.

Rancangan ini selain berpotensi menciptakan tumpang tindih kewenangan dengan pengaturan serupa yang telah ada dalam UU Informasi dan Transaksi Elektronik, juga memberikan ruang yang sangat luas

bagi tindakan penapisan. Dikatakan tindakan penapisan dapat dilakukan terhadap konten/aplikasi yang berbahaya, lalu apa definisi berbahaya? Juga cakupan dan prosedurnya yang akan datur lebih lanjut dengan peraturan BSSN, yang berarti memberikan kewenangan yang sangat besar bagi BSSN. Dari ketentuan ini jelas terlihat bahwa RUU ini gagal menerjemahkan aspek penghormatan terhadap hak asasi manusia, karena dari perumusannya justru berpotensi akan mengancam kebebasan sipil.

Lebih jauh, dengan pemberian kewenangan yang begitu besar, khususnya bagi BSSN dalam pengelolaan keamanan di ruang siber, RUU ini juga sama sekali tidak menghadirkan kerangka pengawasan bagi pelaksanaan kewenangan yang besar tersebut. Akibatnya potensi penyalahgunaan kekuasaannya (*abuse of power*) juga besar, mengingat besarnya kewenangan yang dimiliki untuk mengendalikan segala aspek kehidupan siber di Indonesia.

Dengan beragam catatan dan potensi ancaman di atas, Koalisi Masyarakat Sipil untuk Reformasi Sektor Keamanan menekankan sejumlah hal berikut ini:

1. DPR dan Pemerintah untuk menunda proses pembahasan RUU Keamanan dan Ketahanan Siber pada periode ini, mengingat dari rancangan yang ada sekarang, justru lebih berpotensi mengancam kebebasan sipil. Pemerintah dan DPR harusnya lebih fokus untuk membahas RUU tentang Perlindungan Data Pribadi ketimbang RUU ini. Sebab, RUU Perlindungan Data Pribadi akan memberi jaminan bagi perlindungan warga negara.
2. DPR dan Pemerintah untuk melakukan pengkajian ulang atas kebutuhan keamanan siber, identifikasi aktor dan kebutuhan tiap sektor, perumusan ulang rancangan, serta pelibatan pemangku kepentingan yang lebih luas dalam proses perumusan RUU ini, mengingat besar dan luasnya materi yang akan diatur.
3. Perlunya secara tepat menerjemahkan pendekatan berbasis hak asasi manusia dalam perumusan aturan mengenai keamanan siber, demi menjamin keamanan individu, protokol, perangkat, data, jaringan dan infrastruktur penting lainnya. Bukan sebaliknya, justru mengancam kebebasan sipil dan menciptakan ketidakamanan individu.
4. Negara memegang tanggung jawab penuh untuk melindungi hak dan keamanan warganya, dan bila diperlukan kelompok bisnis dan pemangku kepentingan lainnya dapat terlibat secara konstruktif dan secara kritis, dalam setiap pengembangan dan implementasi kebijakan siber. Oleh karenanya, pengembangan kebijakan dan upaya lain yang dilakukan oleh pemerintah untuk menangani keamanan siber, harus dilakukan secara terbuka dan inklusif, dengan melibatkan seluruh pemangku kepentingan.

B. MENDEFINISIKAN KEAMANAN SIBER: CAKUPAN DAN RUANG LINGKUP

Sampai dengan sekarang, keamanan siber (*cybersecurity*) masih menjadi istilah yang penuh dengan ambiguitas. Semua kalangan membicarakan dan memberikan definisi masing-masing tentang keamanan siber, mulai dari pejabat militer, kepolisian, politisi, pejabat pemerintah, kelompok bisnis, para teknologis, hingga para pengguna internet.¹ Bagi para pengguna internet, keamanan siber akan sangat identik dengan keamanan data pribadi dan keamanan yang terkait dengan aktivitas mereka di internet. Dengan kata lain, keamanan siber berarti kebebasan untuk berinteraksi melalui jaringan internet tanpa ancaman terhadap properti, privasi, atau hak pribadi lainnya. Sementara bagi para politisi dan pejabat (militer, polisi, pemerintah), akan mengidentikakan keamanan siber dengan cakupan keamanan nasional yang lebih luas, termasuk di dalamnya yang terkait erat dengan penyediaan layanan publik. Sedangkan bagi kelompok bisnis, keamanan siber adalah keharusan untuk

¹ Joanna Kulesza & Roy Balleste (eds.), *Cybersecurity and Human Rights in the Age of Cyberteillance*, (London: Rowman & Littlefield, 2016), hal. 13-15.

mengamankan sumber daya mereka secara efektif, baik itu yang berupa ases finansial/moneter juga data-data digital, yang akan menjadi penentu bagi masa depan pengembangan bisnisnya.²

Keamanan siber sendiri adalah disiplin (ilmu) yang relatif baru, sehingga wajar jika sampai dengan sekarang belum ada ejaan yang disepakati atas istilah itu (*cybersecurity* atau *cyber security*), serta belum ada definisi yang disepakati bersama dan diterima secara luas. Definisi ini sendiri dibangun dengan mengacu pada masing-masing spektrum ancaman keamanan siber, yang berarti tindakan apa pun yang akan mengakibatkan akses tidak sah ke suatu perangkat atau sistem, dalam bentuk gangguan, manipulasi, atau kerusakan integritas, kerahasiaan, atau ketersediaan sistem informasi atau informasi yang disimpan, diproses, atau didistribusikan melalui sistem informasi tersebut.³

Beberapa ahli kemudian mendefinisikan keamanan siber adalah sinergi yang disengaja dari teknologi, proses, dan praktik untuk melindungi informasi dan jaringan, sistem dan peralatan komputer, dan program yang digunakan untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi, dari serangan, kerusakan, dan akses tidak sah. Jadi keamanan siber merupakan suatu rangkaian proses kegiatan holistik yang difokuskan pada perlindungan informasi vital suatu organisasi. Keamanan siber mencakup teknologi yang digunakan untuk melindungi informasi, termasuk di dalamnya proses yang digunakan untuk membuat, mengelola, berbagi, dan menyimpan informasi. Juga mencakup praktik-praktik seperti pelatihan dan pengujian sumberdaya manusia untuk memastikan informasi dilindungi dan dikelola dengan baik. Keamanan siber yang efektif harus mampu menjaga kerahasiaan, integritas, dan ketersediaan informasi, melindunginya dari serangan penjahat siber, kerusakan apa pun, dan akses tidak sah oleh mereka yang tidak memiliki akses resmi.⁴

Para ahli keamanan siber umumnya menempatkan keamanan siber pada tiga kategori tujuan umum: (1) kerahasiaan (*confidentiality*); (2) integritas (*integrity*); dan (3) ketersediaan (*availability*), atau sering dikenal sebagai “CIA Triad”. Kerahasiaan mengacu pada upaya pencegahan pengungkapan informasi yang tidak sah, dan sering dikaitkan dengan pelanggaran data karena penyerang berusaha mendapatkan informasi tanpa otorisasi yang tepat. Sedangkan integritas mengacu pada jaminan bahwa pesan yang dikirim sama dengan pesan yang diterima dan bahwa pesan tidak diubah dalam perjalanan. Sedangkan ketersediaan mengacu pada jaminan bahwa informasi akan tersedia bagi konsumen secara tepat waktu dan tanpa gangguan, kapan pun dibutuhkan, terlepas dari lokasi pengguna.⁵

Dengan tiga tujuan utama di atas, Guiora (2017) mendefinisikan keamanan siber sebagai upaya untuk melindungi informasi, komunikasi, dan teknologi dari bahaya yang disebabkan baik secara sengaja maupun tidak sengaja. Selain itu juga penting untuk ditekankan bahwa serangan siber sangat berbeda dari serangan fisik. Lebih jauh menurutnya, keamanan siber adalah upaya untuk memastikan kerahasiaan, integritas, dan ketersediaan data, sumber daya, dan proses melalui penggunaan kontrol administratif, fisik, dan teknis. Sedangkan serangan siber sendiri dimaknai sebagai tindakan agresif yang disengaja dan langsung yang dimaksudkan untuk merusak infrastruktur strategis.⁶

Sedangkan International Telecommunication Union—ITU (2008) sendiri, mendefinisikan keamanan siber sebagai kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman,

² Deborah L. Wheeler, *Understanding Cyber Threats*, dalam Kim Andreasson (ed.), *Cybersecurity Public Sector Threats and Responses*, (New York: CRC Press Taylor & Francis Group, 2012), hal. 29.

³ Thomas A. Johnson, *Cybersecurity Threat Landscape and Future Trends*, dalam *Understanding Cyber Threats*, dalam Kim Andreasson (ed.), *Ibid.*, hal. 287-297.

⁴ Gregory J. Touhill & C. Joseph Touhill, *Cybersecurity for Executives: A Practical Guide*, (New Jersey: John Wiley & Sons, Inc, 2014), hal. 2.

⁵ Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, *Int'l J. Computer Applications Engineering Sci. (Special Issue On Cns)* 257, 257–58 (2011).

⁶ Amos N. Guiora, *Cybersecurity: Geopolitics, law, and policy*, (New York: Routledge, 2017), hal. 16-17.

pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan dan organisasi siber dan aset pengguna. Aset organisasi dan pengguna termasuk perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim dan/atau disimpan dalam lingkungan siber. Keamanan siber berusaha untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan di lingkungan siber.⁷

Dengan sebaran definisi yang demikian, keamanan siber sesungguhnya mengacu pada kemampuan untuk mengontrol akses ke sistem jaringan dan informasi yang dikandungnya. Kontrol keamanan siber yang efektif, menjadi kebutuhan kunci dalam mendukung infrastruktur digital yang handal, tangguh, dan dapat dipercaya.⁸ Apabila suatu negara tidak memiliki otoritas kontrol keamanan siber, atau wewenangnya tidak lengkap, maka diragukan pula kemampuan mereka untuk bisa mengontrol akses jaringan tersebut. Merujuk pada Jennifer L Bayuk, dkk (2012), dalam keamanan siber setidaknya terdapat tiga unsur utama, yang masing-masing unsurnya memiliki beberapa pilar di dalamnya, yaitu: (i) mencegah, mendeteksi, merespon; (ii) orang, proses, teknologi; dan (iii) kerahasiaan, integritas, dan ketersediaan.⁹

C. KONSEPSI UNDANG-UNDANG KEAMANAN SIBER

Ambigu dan ambisiusnya definisi dan cakupan ruang lingkup keamanan siber memang menyulitkan untuk membangun definisi yang lebih solid mengenai keamanan siber, untuk dirumuskan dalam kebijakan keamanan siber suatu negara. Gambaran kebijakan dan strategi keamanan siber diberbagai negara tersebut memperlihatkan beragam dan variatifnya definisi, fokus, serta jangkauan dari kebijakan keamanan siber di tiap-tiap negara. Salah satu problem yang sering mengemuka dalam konteks kebijakan keamanan siber, adalah pemakaian secara bergantian antara keamanan dan kejahatan siber, dengan fokus yang tidak tepat. Seringkali makna dari kedua istilah tersebut cenderung kurang dipahami dengan baik. Saat ini, berbagai negara umumnya mengatur keamanan dan kejahatan siber dalam satu produk regulasi. Alih alih membangun keamanan siber dan secara efektif memberantas kejahatan siber, regulasi-regulasi ini justru acapkali menuai berbagai permasalahan dan rentan disalahgunakan oleh pemerintah untuk melanggar praktik *government surveillance* dan membungkam individu yang mengemukakan kritik terhadap pemerintah—kekuasaan.

Konsepsi keamanan siber sesungguhnya menekankan pada pengimplementasian pendekatan teknis guna mengamankan suatu sistem komputer dari serangan dan kegagalan sistem.¹⁰ Keamanan siber yang baik mengakui bahwa sistem komputer memiliki kerentanan dan berupaya untuk mengatasi akar penyebab ketidakamanan, dengan memprioritaskan pengidentifikasian dan perbaikan kerentanan-kerentanan tersebut.¹¹ Privacy International (2018) mengemukakan bahwa pendekatan terbaik demi mewujudkan keamanan siber yang baik adalah menempatkan individu dan hak-haknya sebagai pusat dari perumusan baik kebijakan maupun strategi keamanan siber, sebagai upaya untuk memperkuat dan melindungi hak asasi manusia.¹² Penempatan individu dan hak-haknya sebagai pusat perumusan kebijakan keamanan siber ini harus diimplementasikan dalam setiap siklus perlindungan, yakni perlindungan terhadap individu, perangkat, dan jaringan.¹³

⁷ Lihat rekomendasi ITU-T X.1205, dapat diakses di <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136>.

⁸ Jennifer L Bayuk, dkk., *Cyber Security Policy Guidebook*, (New Jersey: John Wiley & Sons, Inc), hal. 1.

⁹ Ibid., hal. 3.

¹⁰ Privacy International, *After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security*, 2018, hal.3.

¹¹ Ibid., hal. 3.

¹² Ibid., hal. 4.

¹³ Ibid.

Suatu undang-undang keamanan siber harus mampu dan secara memadai mempertimbangkan dan mengatasi sifat fisik dan virtual dari aset yang akan dilindungi, di samping luasnya cakupan yang begitu kompleks, dengan banyak sisi yang berbeda. Kerangka legislasi keamanan siber harus mampu membedakan tidak hanya aktor-aktor ancaman siber yang berbeda-beda, seperti negara-bangsa, teroris, penjahat, dan peretas jahat, tetapi juga di antara berbagai jenis ancaman siber. Ancaman tersebut termasuk ancaman terhadap infrastruktur strategis, yang dapat menyebabkan hilangnya nyawa atau kerusakan signifikan pada perekonomian suatu negara, serta ancaman terhadap kekayaan intelektual, yang dapat memengaruhi daya saing jangka panjang suatu bangsa.¹⁴

Secara umum pembicaraan mengenai kerangka legislasi keamanan siber mengarah pada panduan yang dirancang untuk menjaga keamanan siber (dengan tiga tujuan). Biasanya merujuk pada peraturan perundang-undangan tentang distribusi informasi, tujuan perusahaan swasta untuk melindungi informasi, metode operasi komputer untuk mengendalikan teknologi, dan variabel konfigurasi dalam perangkat elektronik (Link Gallaher, dkk., 2008). Sederhananya, para ahli bersepakat, bahwa secara umum istilah 'kebijakan keamanan siber' mengacu pada arahan yang dirancang untuk menjaga keamanan siber.¹⁵

Dalam praktiknya memang memperlihatkan adanya pemahaman yang beragam tentang keamanan siber itu sendiri, dan bervariasinya istilah kunci mengenai keamanan siber dari satu negara ke negara lainnya. Perbedaan pemahaman ini mempengaruhi pendekatan yang berbeda dalam penciptaan kebijakan dan strategi keamanan siber negara-negara tersebut. Namun demikian secara umum dapat ditemukan sejumlah titik pertemuan atau poin utama dari kebijakan keamanan siber di setiap negara, yang menggambarkan hal-hal berikut ini:¹⁶

1. Dimaksudkan untuk menentukan kerangka kerja tata kelola keamanan siber;
2. Ditujukan untuk menentukan mekanisme yang tepat, yang memungkinkan semua pemangku kepentingan publik dan swasta yang relevan untuk membahas dan menyepakati kebijakan yang berbeda, termasuk isu-isu dan peraturan yang terkait dengan keamanan siber;
3. Ditujukan untuk menguraikan dan menentukan kebijakan yang diperlukan dan langkah-langkah pengaturan dan peran yang jelas, tanggung jawab dan hak-hak dari sektor swasta dan publik (misalnya kerangka hukum baru untuk memerangi kejahatan siber, pelaporan wajib jika terjadi insiden, langkah-langkah minimum keamanan);
4. Dimaksudkan untuk menetapkan tujuan dan sarana dalam mengembangkan kemampuan nasional dan kerangka hukum yang diperlukan untuk terlibat dalam upaya internasional guna mengurangi efek dari kejahatan siber;
5. Mengidentifikasi infrastruktur informasi penting termasuk aset utama, layanan dan saling ketergantungan;
6. Ditujukan untuk mengembangkan atau meningkatkan kesiapsiagaan, respon dan rencana pemulihan dan langkah-langkah untuk melindungi infrastruktur informasi yang penting (misalnya rencana darurat nasional, latihan siber, dan kesadaran situasi);
7. Menentukan pendekatan yang sistematis dan terintegrasi bagi manajemen risiko nasional;
8. Menentukan dan menetapkan tujuan untuk kampanye peningkatan kesadaran guna menanamkan perubahan perilaku dan pola kerja pengguna;

¹⁴ Contreras, J. L., DeNardis, L. and Teplinsky, M. June 2013. "America the Virtual: Security, Privacy, and Interoperability in an Interconnected World: Foreword: Mapping Today's Cybersecurity Landscape." *American University of Law Review*, 48.

¹⁵ Selengkapnya lihat: M. P., A. N. Link Gallaher, et al., *Cyber Security, Economic Strategies and Public Policy Alternatives*. Cheltenham, UK: Edward Elgar, 2008.

¹⁶ Lihat: Cyber Security Strategy Documents, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), update 17 February 2016, dan European Network and Information Security Agency (ENISA).

9. Menentukan kebutuhan kurikulum baru dengan penekanan pada keamanan siber bagi praktisi dan spesialis keamanan teknologi informasi, dan juga pelatihan program yang memungkinkan peningkatan keterampilan pengguna;
10. Kerjasama internasional, serta program penelitian dan pengembangan komprehensif yang berfokus pada isu-isu keamanan dan ketahanan.

Dengan beragam materi di atas, sebuah undang-undang keamanan siber pada intinya bertujuan untuk meningkatkan ketahanan siber suatu negara. Namun demikian, untuk memastikan hal itu, beberapa poin penting yang harus diperhatikan pada saat proses perancangan kerangka kerja—kebijakan keamanan siber, materi yang harus dimunculkan adalah berikut ini:¹⁷

- Regulasi dan Kebijakan

UU Keamanan siber memberikan mandat bagi pemerintah untuk menyusun kebijakan berupa panduan, seperti Strategi Keamanan Siber Nasional, atau Kebijakan TIK, yang menetapkan visi suatu negara di masa depan, yang juga berfungsi sebagai panduan untuk memprioritaskan isu di bidang keamanan siber.

- Mengidentifikasi dan Memprioritaskan Keamanan dari Infrastruktur Kritis Negara

Dalam praktiknya, negara memiliki definisi tersendiri mengenai ruang lingkup infrastruktur kritis negara. Sebagai contoh, Uni Eropa mendefinisikan infrastruktur kritis sebagai sebuah aset, sistem atau bagian darinya, yang bersifat esensial dalam pemeliharaan fungsi-fungsi sosial yang vital, kesehatan, keselamatan, keamanan, kesejahteraan ekonomi atau sosial manusia, dan gangguan atau penghancuran yang akan memiliki dampak signifikan sebagai akibat dari kegagalan untuk mempertahankan fungsi-fungsi tersebut.¹⁸

The European Union Network Information Security (NIS) Directive (2016) misalnya mengidentifikasi layanan-layanan yang dianggap esensial sehingga harus dilindungi sebagai infrastruktur kritis, yakni, energi (listrik, minyak, gas) transportasi (udara, rel, air, jalan), infrastruktur pasar finansial perbankan, kesehatan, hingga infrastruktur digital.¹⁹ Setelah infrastruktur kritis dapat diidentifikasi, langkah selanjutnya yang seharusnya dilakukan oleh Pemerintah adalah menyusun regulasi guna memastikan perlindungan infrastruktur kritis tersebut, seperti standar keselamatan minimum, mekanisme untuk melaporkan pelanggaran keamanan, dan rencana untuk respons dan pemulihan insiden siber.

- Membentuk Tim yang Didedikasikan untuk Merespon Insiden Siber

Pendirian tim yang secara khusus bertugas untuk merespon insiden siber adalah salah satu hal penting dalam rencana respons dan pemulihan insiden siber. Dalam praktiknya, terdapat banyak jenis tim respon insiden siber, beberapa memiliki tanggung jawab nasional, dan beberapa spesifik untuk sektor tertentu. Contoh tim respon insiden siber yang paling kerap dijumpai adalah Tim Tanggap Insiden Keamanan Siber atau *The Cyber Security Incident Response Team* (CSIRT), yang menangani insiden keamanan yang terjadi pada infrastruktur teknologi informasi dan komunikasi.

- Melakukan Penilaian Ancaman (*Threat Assessment*) dan Mengembangkan Rencana Pemulihan

¹⁷ Privacy International, Op.Cit, hal. 9-12.

¹⁸ Council Directive 2008/114/EC, Article 2.

¹⁹ DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>.

Pelaksanaan penilaian ancaman bertujuan untuk mengidentifikasi kemungkinan kelemahan, seperti infrastruktur yang ketinggalan zaman, yang membuat negara menjadi lebih rentan terhadap serangan siber. Penilaian ancaman ini membantu mengalokasikan sumber daya secara efektif untuk mengatasi ancaman paling akut. Umumnya, CSIRTS merupakan pihak yang bertugas dalam pembuatan penilaian ini. Pendekatan yang digunakan dalam menyusun regulasi keamanan siber haruslah bersifat "defensif". Hal ini berarti bahwa regulasi keamanan siber idealnya berisi mengenai tindakan untuk mengamankan sistem dari serangan. Pengadopsian pendekatan "ofensif" dalam regulasi keamanan siber hanya akan menyebabkan maraknya praktik *surveillance* oleh pemerintah serta tindakan ofensif lainnya terhadap hak asasi manusia warga negara.

D. PROBLEM RUU KEAMANAN DAN KETAHANAN SIBER

- Definisi, Asas dan Tujuan

RUU ini secara limitatif telah memberikan definisi mengenai siber, keamanan dan ketahanan siber, kepentingan siber, dan ancaman siber.

Dalam RUU ini dikatakan (Pasal 1 angka 1), siber adalah ruang yang bersifat global dan mewadahi aneka ragam kepentingan yang dibentuk dari interaksi antara manusia dengan teknologi informasi, komputerisasi, jaringan computer, kriptografi, dan/atau kecerdasan buatan. Pemberian definisi yang limitatif terhadap siber ini justru telah keluar dari corak dan karakteristik siber itu sendiri, yang sangat inovatif dan luasangkauannya. Akibatnya, dengan pemberian definisi ini hukum akan semakin lebih cepat usang dan tidak mampu memfasilitasi setiap perkembangan dari ruang siber.

Seharusnya kerangka hukum yang dibuat harus sejalan dengan cepatnya inovasi teknologi, sehingga dia perlu bersifat supel, yang berarti mampu mengantisipasi setiap perubahan di masa depan, dengan memberikan standar yang fleksibel dan dapat berlaku bagi semua perkembangan teknologi. Dengan aturan yang tidak kaku, hukum akan mampu memberikan ruang untuk setiap invensi dan inovasi teknologi, serta dapat secara baik memfasilitasi pengembangan berbasis digital.

Sementara terkait dengan definisi keamanan dan ketahanan siber, catatan utamanya adalah kegagalannya di dalam mengidentifikasi elemen-elemen kunci yang semestinya ada dalam definisi keamanan siber. Lepas dari belum adanya kesamaan definisi dari keamanan siber di seluruh dunia, akan tetapi semestinya beberapa unsur penting seperti kerahasiaan, integritas, dan ketersediaan dapat terakomodasi di dalam definisi keamanan siber. Definisi keamanan siber yang dibangun dalam RUU ini justru memperlihatkan definisi yang sifatnya state centric, karena penekanannya bukan pada keamanan system siber itu sendiri. Ini mengemuka dikarenakan jika dilacak lebih jauh, rujukan definisi mengacu pada definisi keamanan nasional, yang dirumuskan dalam RUU Keamanan Nasional inisiatif pemerintah, yang sampai hari ini belum dibahas di DPR.

Sedangkan definisi kepentingan siber dan ancaman siber, dalam RUU ini sepenuhnya mengacu pada definisi kepentingan nasional dan ancaman yang dirumuskan oleh UU No. 17/2011 tentang Intelijen Negara. Padahal maksud dan tujuan antara UU Intelijen Negara dan aturan tentang keamanan siber semestinya penekanannya berbeda. Lagi-lagi adopsi definisi ini justru kian menguatkan pendekatan yang lebih state centric pada RUU Keamanan dan Ketahanan Siber ini.

Titik tekan pada kedaulatan yang identik dengan terminology kedaulatan tradisional, terkait dengan teritorial dan yurisdiksi, juga menjadikan RUU ini menjadi tak-sejalan dengan sifat alamaiah dari siber yang lintas batas. Berbicara tentang kedaulatan di ruang siber, semestinya penekanannya pada kedaulatan individu di ruang siber, yang hak-haknya dilindungi dengan seperangkat instrument perlindungan. Oleh karenanya asas yang perlu dikembangkan semestinya bukan kedaulatan, tetapi

justru berbasis pada manusia atau *human centric approach*, yang menekankan pada keamanan individu di ruang siber. Penekanan pada aspek kedaulatan negara (territorial dan yurisdiksi) ini juga mengemuka pada identifikasi tujuan yang dirumuskan oleh RUU ini, yang jelas menyatakan bertujuan untuk melindungi keutuhan dan kedaulatan negara dari ancaman siber. Justru aspek keamanan individu, perangkat, dan jaringan sama sekali tidak rumuskan sebagai bagian yang utama dari keamanan siber itu sendiri.

- **Penyelenggara Keamanan dan Ketahanan Siber**

Dari rumusan yang ada, RUU ini belum mampu untuk mengakomodasi pendekatan multi-pemangku kepentingan dalam keamanan siber, yang nampak secara eksplisit dari identifikasi aktor-aktor penyelenggara keamanan siber. Dikatakan penyelenggara keamanan dan ketahanan siber adalah lembaga negara, pemerintah pusat, pemerintah daerah, dan masyarakat (Pasal 3). Sementara posisi korporasi/bisnis yang memegang peran kunci dalam keamanan siber, khususnya dari perangkat dan jaringan yang mereka kelola, termasuk individu konsumen mereka, justru tidak teridentifikasi. Bahkan dalam ketentuan berikutnya (Pasal 6), penyelenggara keamanan dan ketahanan siber hanya disebutkan lembaga negara, pemerintah pusat, dan pemerintah daerah, yang kembali menegaskan bahwa RUU ini menghendaki pengelolaan urusan keamanan siber hanya akan menjadi domain dari negara atau bahkan pemerintah.

Padahal sebuah kebijakan keamanan siber seharusnya secara jelas menentukan mekanisme yang tepat, yang memungkinkan semua pemangku kepentingan publik dan swasta yang relevan untuk membahas dan menyepakati kebijakan yang berbeda, termasuk isu-isu dan peraturan/regulasi yang terkait dengan keamanan siber. Selain itu, dia juga harus mampu menguraikan dan menentukan kebijakan yang diperlukan dan langkah-langkah pengaturan dan peran yang jelas, tanggung jawab dan hak-hak dari sektor swasta dan publik (misalnya kerangka hukum baru untuk memerangi *cybercrime*, pelaporan wajib jika terjadi insiden, langkah-langkah minimum keamanan). Dengan rumusan yang ada sekarang, justru akan menciptakan banyak ambiguitas dan besarnya potensi tumpang tindih kewenangan, bahkan sengketa kewenangan antar aktor yang menyelenggarakan keamanan dan ketahanan siber. Belum lagi pemberian sejumlah kewenangan baru bagi BSSN, dimana wewenang tersebut sudah dikerjakan operasionalnya oleh sejumlah kementerian/lembaga lainnya, misalnya: fungsi deteksi dini melalui intelligent signal yang sudah dilakukan oleh Badan Intelijen Negara (BIN), pemberian sertifikasi elektronik dan pelaksanaan penapisan konten yang sudah diselenggarakan oleh Kemkominfo, fungsi investigasi yang menjadi kewenangan dari kepolisian, dan kerja-kerja diplomasi siber yang secara rutin telah dilakukan dan dikoordinasikan oleh Kementerian Luar Negeri.

- **Tata Kelola Keamanan dan Ketahanan Siber**

Sebuah undang-undang keamanan siber yang baik harus mampu mengidentifikasi infrastruktur informasi penting termasuk aset utama, layanan dan saling ketergantungannya. Selain itu dia juga harus secara tepat menentukan pendekatan yang sistematis dan terintegrasi bagi manajemen risiko nasional. Sedangkan RUU Keamanan dan Ketahanan Siber meski menyebutkan operasionalisasi keamanan siber untuk mengamankan infrastruktur siber nasional, termasuk di dalamnya infrastruktur informasi kritikal nasional, namun tidak memberikan kejelasan mengenai definisi dan cakupannya (Pasal 10 ayat (2)). Secara delegatif, rumusan yang dibangun dalam pengaturan ini juga problematis, oleh karena hal-hal yang seharusnya diatur oleh Peraturan Presiden sebagai kepala pemerintahan tertinggi, atau bahkan pada level peraturan pemerintah, justru akan diatur pada level peraturan Lembaga (Pasal 10 ayat (4)).

Hal ini misalnya nampak dari rumusan pasal yang terkait dengan identifikasi ancaman siber. Dalam ketentuan Pasal 11 ayat (2) disebutkan bahwa ancaman siber terdiri dari: *a. Insiden Siber yang terjadi*

dalam Perimeter Keamanan; b. Serangan Siber terhadap Objek Pengamanan Siber; c. perangkat lunak yang berbahaya; d. konten yang mengandung muatan destruktif dan/atau negative; e. produk, prototype produk, rancangan produk, atau invensi yang dapat digunakan sebagai senjata siber; f. upaya yang sengaja ditujukan untuk melemahkan, merugikan, dan/atau menghancurkan kepentingan siber Indonesia; dan/atau bentuk ancaman siber lainnya.

Identifikasi ancaman tersebut mengandung sejumlah kelemahan dan justru berpotensi mengancam kebebasan sipil, misalnya penempatan konten yang mengandung muatan destruktif dan/atau negative sebagai ancaman siber. Rumusan ini menjadi penuh dengan ketidakpastian dan bisa menjadi instrumen pembatasan untuk membatasi berbagai macam konten di dunia internet, dengan tuduhan destruktif atau negative. Selain itu identifikasi ancaman tersebut juga dapat menghambat pengembangan pengetahuan dalam bentuk invensi dan inovasi siber, termasuk di dalamnya pengembangan persenjataan siber, yang semestinya menjadi bagian penting dari pengembangan industri strategis nasional. Potensi hambatan dalam inovasi menjadi kian menguat dengan adanya birokratisasi perijinan penelitian yang terkait dengan keamanan siber, sebagaimana diatur Pasal 48 huruf f, yang memberikan wewenang bagi BSSN untuk mengelola izin penelitian dan pengujian kekuatan keamanan siber. Lebih parahnya, jika terjadi gangguan sistem sebagai akibat dari suatu kegiatan penelitian atau pengujian kekuatan keamanan siber, yang tidak memiliki ijin dari BSSN, dikenakan ancaman pidana 10 (sepuluh) tahun penjara dan/atau denda 10 miliar rupiah (Pasal 71).

Selain problem tersebut, dalam konteks tata kelola keamanan dan ketahanan siber, juga besar terjadi potensi tumpang tindih kewenangan antar-lembaga. Hal ini misalnya tercermin dari adanya pengaturan mengenai sertifikasi perangkat siber yang dituangkan dalam ketentuan Pasal 17. Potensi tumpang tindih kewenangan terutama terkait dengan penyelenggaraan sertifikasi elektronik, yang sebelumnya telah diatur di dalam ketentuan UU No. 11/2008 tentang Informasi dan Transaksi Elektronik. Lebih jauh, potensi benturan kewenangan antar-lembaga juga terjadi, terutama dalam aspek penegakan tata kelola, yang diatur dalam ketentuan Pasal 22. Dalam UU ini diatur bahwa penyelenggara keamanan dan ketahanan siber adalah: lembaga negara, pemerintah pusat, dan pemerintah daerah, artinya keseluruhannya adalah lembaga pemerintah. Sementara dalam penegakan tata kelola, dibuka peluang pemberian sanksi, dari teguran hingga penghentian/pemblokiran permanen operasional sistem elektronik, juga penerapan denda administratif. Pun demikian dengan ketentuan Pasal 23 dan Pasal 24, yang juga memberikan ancaman sanksi dalam penegakan tata kelola. Artinya, apakah sesama lembaga pemerintah akan menerapkan sanksi pada lembaga pemerintah yang lain? Bagaimana mekanismenya?

Dalam risiko kerugian dan pertanggungjawaban kerugian, juga ada ketidaktepatan dalam perumusan skema restitusi, kompensasi, dan rehabilitasi (Pasal 28), yang justru menjadi pasal tanpa makna. Mengapa tidak tepat? Sebab dalam hukum Indonesia, skema pemberian kompensasi/restitusi/rehabilitasi hanya berlaku bagi kejahatan tertentu, misalnya pelanggaran hak asasi manusia yang berat, tindak pidana terorisme, tindak pidana perdagangan orang, tindak pidana penyiksaan dan penganiayaan berat (lihat UU Perlindungan Saksi dan Korban). Sedangkan keamanan siber bukanlah bagian dari skema tersebut, kendati perbuatannya masuk kualifikasi kejahatan siber sekalipun, sehingga keberadaan pasal itu belum menjawab kebutuhan mekanisme koreksi dan pemulihan dari sebuah UU keamanan siber. Usulan RUU ini juga sama sekali belum menghadirkan skema pengawasan, baik yang dilakukan secara melekat maupun adhoc, dalam implementasi dan operasionalisasi keamanan siber.

- Problem Hak Asasi Manusia

Ketentuan Pasal 5 huruf b RUU ini memang menegaskan bahwa dalam penyelenggaraan keamanan dan ketahanan siber salah satunya harus mengedepankan penghormatan hak asasi manusia. Namun dalam rumusannya justru muncul sejumlah materi yang lebih menekankan pada aspek pembatasan

atau cenderung akan mengancam jaminan perlindungan kebebasan sipil itu sendiri. Problem pembatasan ini misalnya mengemuka dari luasnya definisi dan cakupan ruang lingkup ancaman siber, yang diatur pada Pasal 11 ayat (2), sebagaimana di bahas sebelumnya di atas. Padahal dalam laporannya, Pelapor Khusus PBB untuk Kebebasan Berpendapat dan Berekspresi, menegaskan: negara seharusnya hanya berusaha untuk membatasi konten sesuai dengan perintah oleh otoritas kehakiman yang independen, sesuai dengan proses dan standar legalitas, keperluan dan legitimasi.

Problem pembatasan tersebut menjadi kian eksplisit dengan adanya rumusan pasal mengenai penapisan konten dan aplikasi elektronik, terhadap konten dan aplikasi yang dinilai berbahaya (Pasal 38). Rumusan ini tentu sangat jauh dari sandaran pembatasan yang dikembangkan dalam hukum internasional hak asasi manusia, yang menghendaki tiga tahapan tes ketika pembatasan konten akan dilakukan: diatur oleh hukum, untuk suatu tujuan yang sah atas nama: keamanan nasional, keamanan publik, moral publik, kesehatan publik, ketertiban umum, serta hak dan reputasi orang lain; dan pembatasan itu memang sangat diperlukan, dengan melalui cara-cara yang proporsional. Alasan bahaya sama sekali tidak dikenal dalam hukum internasional hak asasi manusia, dan akan sangat multitafsir dalam penerapannya, yang justru lebih besar potensinya bagi kebebasan sipil. Meski konten dan aplikasi dapat dibatasi, namun selain ada kejelasan dasar hukum, juga harus ada kejelasan prosedur yang diatur dalam hukum yang menyatakan pembatasan itu. Sedangkan rumusan dalam RUU ini sama sekali tidak mengatur mengenai prosedur dilakukannya pembatasan konten dan aplikasi tersebut.

Pembentukan pusat operasi keamanan dan ketahanan siber bagi semua penyelenggara—keamanan siber, yang terkoneksi dengan pusat operasi siber nasional, juga mengancam perlindungan hak atas privasi pengguna internet—public (Pasal 31). Besarnya potensi ancaman terhadap privasi, khususnya data pribadi dan komunikasi pribadi ini, sebab koneksi pusat operasi tersebut memungkinkan monitoring lalu lintas data dan internet, oleh lembaga yang mengelola pusat operasi siber nasional. Potensi ini nampak kian nyata dengan adanya usulan mengenai kewenangan BSSN untuk melakukan deteksi ancaman siber pada lalu lintas data (Pasal 47 dan Pasal 48). Padahal, Pelapor Khusus PBB untuk Kebebasan Berpendapat dan Berekspresi sekali lagi menegaskan, negara dan organisasi antar pemerintah harus menahan diri dari menetapkan undang-undang atau pengaturan yang akan membuka kemungkinan dan kewenangan pemantauan "proaktif" atau penyaringan konten, karena tidak sejalan dengan perlindungan hak atas privasi.
