KLIPING PERPUSTAKAAN DPR-RI
http://kliping.dpr.go.id

Judul : Pakar Ungkap 22 Titik Buta dalam RUU KKS
Tanggal : Rabu, 01 Juli 2026
Surat Kabar : Kompas
Halaman : 4

KETAHANAN SIBER

Pakar Ungkap 22 Titik Buta dalam RUU KKS

JAKARTA, KOMPAS — Pemerintah dan DPR diminta untuk tidak tergesa-gesa membahas Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber atau RUU KKS. Substansi RUU KKS belum menjawab kompleksitas ancaman siber yang terus berkembang, bahkan masih terdapat 22 titik buta (*blind spot*) yang belum terakomodasi dalam rumusan regulasi yang disusun pemerintah tersebut.

Pembahasan RUU Keamanan dan Ketahanan Siber antara pemerintah dan DPR mulai bergulir, Senin (29/6/2026). Komisi I DPR telah membentuk panitia kerja setelah menerima usulan draf RUU dan naskah akademik dari pemerintah. Fraksi-fraksi di Komisi I DPR juga telah menyampaikan daftar inventarisasi masalah.

Sehari kemudian, Selasa (30/6), Komisi I menggelar rapat dengar pendapat umum dengan pendiri Indonesia Cybersecurity Forum (ICSF), Ardi Sutedja, serta Direktur Eksekutif Cyber Communication and Information System Security Research Center (CISSReC) Pratama Persadha untuk meminta masukan terhadap RUU tersebut.

Dalam rapat itu, Ardi mengingatkan bahwa ancaman siber seperti gunung es. Namun, pemahaman negara terhadap ancaman siber saat ini baru menyentuh sebagian kecil persoalan yang sebenarnya.

"Kita mungkin terjebak dalam fenomena *iceberg of ignorance* atau gunung es ketidaktahuan. Yang kita pahami sebetulnya hanya 4 persen di permukaan. Padahal, ancaman siber yang paling besar berada di bawah permukaan," ujarnya.

Menurut dia, pola serangan siber kini semakin sulit dideteksi, terlebih dengan perkembangan kecerdasan artifisial dan teknologi kuantum yang berlangsung sangat cepat. Di sisi lain, Indonesia dinilai belum memiliki kemandirian teknologi yang memadai untuk menghadapi ancaman tersebut.

Karena itu, Ardi mengingatkan, pembentukan RUU KKS tidak boleh dilakukan secara tergesa-gesa. Berdasarkan kajian ICSF, sedikitnya terdapat 22 titik buta yang belum terakomodasi dalam draf pemerintah. Kekurangan itu mencakup landasan filosofis, ruang lingkup pengaturan, manajemen krisis, perlindungan hak privasi, hingga diplomasi siber.

> ***Perlu kita perjelas kalau misal terjadi serangan yang besar, siapa yang memimpin.***
> Pratama Persadha

Berbagai persoalan mendasar tersebut, katanya, masih perlu dibahas lebih komprehensif dengan melibatkan unsur masyarakat, akademisi, dan pelaku industri. Ia mendukung pembahasan RUU dilanjutkan, tetapi meminta pemerintah dan DPR tidak terburu-buru mengesahkannya.

"Jangan terburu-buru membahas dan mengesahkannya menjadi undang-undang karena banyak aspek belum tergali dan belum ada sosialisasi yang matang dengan masyarakat dan industri," ujarnya.

Kelemahan tata kelola

Selain substansi regulasi, Ardi menilai Indonesia masih menghadapi persoalan mendasar berupa kesenjangan sumber daya manusia di bidang keamanan siber. Ketika terjadi insiden, banyak institusi justru tidak mengetahui langkah yang harus dilakukan atau mengalami *frozen action*.

Persoalan lain ialah tata kelola data pemerintah yang belum terintegrasi. Ribuan aplikasi dikembangkan kementerian dan lembaga tanpa koordinasi sehingga tidak saling terhubung. Kondisi tersebut dinilai memperbesar risiko kebocoran data.

Pratama Persadha menyampaikan pandangan serupa. Menurut dia, setiap kali terjadi insiden siber, para pihak justru sibuk saling menyalahkan karena tidak ada pembagian kewenangan yang jelas antarlembaga. Padahal, keberhasilan penanganan insiden sangat bergantung pada kejelasan peran setiap institusi.

"Nah, oleh karena itu, menurut saya, perlu kita perjelas kalau misal terjadi serangan yang besar, siapa yang memimpin, siapa yang menyelidiki, siapa yang menangani pemulihan, siapa yang memberikan informasi kepada publik, kapan Presiden menerima laporan, kapan status krisis nasional ditetapkan, dan bagaimana koordinasi lintas kementerian atau lembaga dan sektor swasta," katanya.

Pratama juga menilai aspek ketahanan siber (*cyber resilience*) jauh lebih penting daripada sekadar keamanan siber (*cyber security*). Ia menambahkan, keamanan siber berfokus pada pencegahan serangan, sedangkan ketahanan siber menitikberatkan kemampuan sistem untuk tetap beroperasi dan pulih setelah mengalami serangan.

Meski demikian, aspek ketahanan siber masih sangat minim diatur dalam draf RUU pemerintah. Oleh karena itu, ia mengusulkan agar seluruh infrastruktur informasi kritis diwajibkan memiliki *business continuity plan* dan *disaster recovery plan*.

Sementara itu, sebelumnya, dalam rapat bersama pemerintah, Senin, Ketua Komisi I DPR Utut Adianto meminta agar draf RUU KKS tidak disebarluaskan kepada publik pada tahap awal pembahasan. Menurut dia, penyebarluasan draf berpotensi memunculkan hoaks.

Utut juga meminta pemerintah membentuk tim pembahas yang kuat agar pembahasan RUU berjalan optimal. "Tim yang rajin. Rajin itu penting, Pak, karena biasanya pembahasan seperti ini sangat menjemukan," katanya. (BOW)