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

Judul : Garap RUU KKS, komisi I fokus lindungi ruang privat masyarakat
Tanggal : Jumat, 09 Oktober 2026
Surat Kabar : Rakyat Merdeka
Halaman : 3

Garap RUU KKS

Komisi I Fokus Lindungi Ruang Privat Masyarakat

KOMISI I DPR tengah menggarap Rancangan Undang-Undang (RUU) Keamanan dan Ketahanan Siber (KKS). Regulasi itu akan memuat kejelasan norma serta pembagian tanggung jawab antarlembaga agar mampu menjaga perlindungan hak privat warga secara optimal.

Anggota Komisi I DPR Sarifah Ainun Jariyah mengatakan, desain pengawasan dalam RUU KKS kudu diperjelas. Negara memang membutuhkan kewenangan memantau anomali trafik siber untuk keamanan nasional. Namun kewenangan itu wajib disertai mekanisme pengawasan kuat, agar tidak menimbulkan celah pelanggaran privasi bagi seluruh warga negara.

Sarifah menilai persoalan pengawasan siber ini jadi semakin mendesak sebab ancaman memiliki karakter cepat serta berlangsung secara *real-time*. Mekanisme pengawasan tidak boleh dirancang terlalu panjang. "Aturan berbelit bisa menghambat Pemerintah merespons tiap serangan maupun anomali siber yang muncul dengan cepat," terangnya, Rabu (7/10/2026).

Dia berharap ada penjelasan konkret soal konsep pengawasan independen terhadap pemantauan siber oleh negara. Mesti ada kepastian, apakah pemantauan wajib memerlukan izin pengadilan terlebih dulu atau cukup memakai mekanisme *post-factum review* pada kondisi tertentu.

Untuk itu, Sarifah meminta kalangan akademisi memberikan gambaran mengenai model pengawasan independent yang paling tepat untuk diterapkan. Opsi yang dikaji mencakup pembentukan lembaga independen khusus atau memanfaatkan lembaga yang sudah ada. Alternatif lainnya adalah mengembangkan skema pengawasan internal pada masing-masing institusi terkait secara efektif.

Dia mendorong adanya studi banding dari negara lain yang telah memiliki mekanisme pengawasan siber. Langkah itu diambil agar Indonesia tidak merumuskan norma tanpa mempertimbangkan praktik internasional. "Kajian mencakup penentuan negara rujukan paling relevan, skema pengawasan, serta pelajaran untuk merumuskan norma RUU KKS," ujarnya.

Sarifah juga menyoroti perlindungan hukum penyedia sistem yang melaporkan insiden maupun anomali siber. Pihaknya meminta masukan dari pelaku industri serta asosiasi seperti Indonesia Data Center Provider Organization (IDPRO) dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Karnea, industri memahami langsung persoalan operasional dan risiko hukum dari insiden siber.

Dia lalu menyinggung rekomendasi klausul *safe harbor* dalam matriks RUU KKS serta masukan integrasi pelaporan insiden dari sektor industri. Kewajiban pelaporan wajib dirancang

FOTO: FB PRIBADI

Sarifah Ainun

tanpa menimbulkan ketakutan bagi penyedia sistem. "Pihak penyedia yang jadi solusi jangan sampai enggan melapor karena khawatir ancaman sanksi hukum," tegasnya.

Sarifah meminta agar RUU KKS memberikan kepastian hukum bagi penyedia sistem yang melaporkan insiden secara cepat, jujur, transparan, dan beritikad baik. Norma perlindungan perlu menegaskan laporan tidak dijadikan dasar pemidanaan atau sanksi administratif, sepanjang tidak ada unsur kesengajaan maupun manipulasi fakta material.

Sejalan dengan itu, anggota Komisi I DPR Amelia Anggraini menyoroti kejelasan norma serta pembagian tanggung jawab dalam RUU KKS. Rumusannya wajib bisa dilaksanakan pelaku industri dan memberi perlindungan maksimal bagi masyarakat. Perlu ada masukan konkret mengenai parameter penetapan infrastruktur kritikal, termasuk data center dan cloud.

Dia mengingatkan agar kriteria penetapan infrastruktur itu dirumuskan secara terukur. Penetapannya tidak boleh terlalu luas hingga semua fasilitas dianggap kritikal. "Kriterianya juga jangan terlalu sempit agar infrastruktur utama yang jadi penyokong banyak sektor tidak terabaikan tanpa sistem perlindungan hukum yang memadai," ingatnya.

Pembagian tanggung jawab bersama dalam ekosistem digital mencakup pemilik data center, penyedia *cloud*, Penyelenggara Sistem Elektronik, serta pengelola aplikasi. Batas kewenangan wajib ditegaskan agar tidak saling melempar tanggung jawab saat terjadi serangan siber. Makanya, regulasi ini perlu memperjelas perbedaan pasal UU dengan aturan teknis turunannya.

Soal aturan safe harbor, Amelia menggarisbawahi soal perlindungan pada keterbukaan informasi bagi pelapor insiden maupun penemu kerentanan siber beritikad baik. Karena tanpa perlindungan, keterbukaan informasi ancaman akan terhambat. "Desain aturan wajib dibuat tepat agar tidak jadi celah berlindung bagi perusahaan yang melakukan kelalaian operasional," tuturnya.

Menyikapi hal itu, Dewan Penasihat IDPRO Kalamullah Ramli memaparkan praktik pengawasan siber di beberapa negara. Di China, pemerintahnya menerapkan sistem Great Firewall tanpa kontrol independen masyarakat. Sedangkan Rusia memiliki skema Sistem Tindakan Penyelidikan Operasional melalui UU Yarovaya, tapi pengawasannya lemah akibat akses aparat tanpa izin.

Kemudian, AS menerapkan penyadapan kriminal melalui Wiretap Act yang membutuhkan surat perintah hakim. Pengawasan trafik dilakukan per program dengan persetujuan pengadilan khusus sesuai Pasal 702 setiap tahun. Mekanisme ini memungkinkan penyadapan secara luas terhadap program ancaman tertentu seperti tindakan terorisme maupun negara lawan.

Selanjutnya India mengatur sistem pemantauan terpusat melalui UU ITE dan UU Telegraf. Pemantauan memerlukan izin dari pihak eksekutif seperti Sekretaris Dalam Negeri serta komite peninjau internal. "Lembaga pengawas di negara itu diisi komite independen nonhakim untuk mengevaluasi seluruh pelaksanaan pemantauan siber nasional," paparnya.

Sementara Ketua Umum APJII Muhammad Arif mengungkapkan kekhawatiran pelaku usaha terkait pemutusan akses internet tanpa perintah tertulis. Permintaan lisan dari kementerian sering diterima tanpa adanya payung hukum yang jelas. Situasi itu menimbulkan dilema keamanan operasional serta risiko fisik bagi para penyelenggara jasa internet. ■ PYB