CIPS
Center for Indonesian Policy Studies

RINGKASAN KEBIJAKAN

Maret 2021

Ringkasan Kebijakan No. 9

Perlindungan Keamanan Siber di Indonesia

oleh Noor Halimah Anjani

Pesan Utama

- Pada 2019, Badan Siber dan Sandi Negara (BSSN) melaporkan 290 juta kasus serangan siber. Jumlah tersebut 25% lebih banyak jika dibandingkan tahun sebelumnya ketika kejahatan siber menyebabkan kerugian sebesar US$ 34,2 miliar di Indonesia. Pandemi Covid-19, selain memicu peningkatan serangan *phising* (pengelabuan), serangan *malware spams* dan *ransomware* yang signifikan, juga meningkatkan desakan untuk menetapkan infrastruktur keamanan siber yang berfungsi dengan baik.

- Undang-Undang (UU) dan peraturan-peraturan yang berkaitan dengan keamanan siber di Indonesia membagi tanggung jawab ke beberapa kementerian dan hal itu dinilai tidak efektif dalam mencegah ancaman dan kejahatan siber. Oleh karena itu, sebuah peraturan yang komprehensif untuk keamanan siber sangat dibutuhkan di Indonesia.

- Anggota Dewan Perwakilan Rakyat (DPR) Republik Indonesia telah mendiskusikan Rancangan Undang-Undang (UU) Keamanan Siber secara menyeluruh, namun prosesnya tidak melibatkan pihak swasta. Akibatnya, RUU tersebut mengandung aturan yang menyulitkan dan merugikan pengusaha, seperti adanya kewajiban sertifikasi, akreditasi, dan persetujuan dari BSSN untuk mengembangkan layanan dan produk. Selain itu, persyaratan kandungan lokal juga menambah risiko keamanan siber Indonesia. RUU ini dikritik keras dan kemudian dikeluarkan dari Program Legislasi Nasional tahun 2020 dan 2021.

- RUU Keamanan Siber yang direvisi harus dengan jelas mendefinisikan dan menjabarkan peran, tanggung jawab, dan otoritas lembaga terkait dalam mengatasi ancaman keamanan siber.

- DPR dan BSSN harus terlibat dalam dialog antara Pemerintah dan Swasta atau *Public-Private Dialogue* (PPD) ketika mendiskusikan RUU ini. PPD terbukti membantu pertukaran informasi dan pengalaman yang relevan, membuat kebijakan yang lebih tepat sasaran dan bisa dilaksanakan dengan baik, serta didukung oleh pemangku kepentingan secara luas.

Kondisi Keamanan Siber di Indonesia

Dalam beberapa dekade terakhir, perkembangan teknologi informasi dan komunikasi secara positif telah berkontribusi terhadap perkembangan ekonomi global dan berdampak pada produktivitas, persaingan, dan keterlibatan warga negara yang lebih tinggi (Setiadi, Sucahyo, & Hasibuan, 2012). Akan tetapi, karena badan pemerintah, pengusaha, dan masyarakat kini jauh lebih terkoneksi di dunia maya, beberapa tantangan terkait ancaman siber membutuhkan lebih banyak perhatian untuk mengembangkan keamanan siber yang lebih kuat.

Keamanan siber terdiri dari praktik, tindakan-tindakan, dan upaya-upaya yang melindungi ekosistem siber dan aset-aset perusahaan dan pengguna dari serangan berbahaya yang bertujuan untuk mengganggu kerahasiaan, integritas, dan ketersediaan informasi atau data (Fischer, 2005; ITU, 2012). Aset-aset yang dimaksud, termasuk tapi tidak terbatas pada, perangkat komputasi yang saling terhubung, infrastruktur penting, server, jaringan, dan informasi yang disimpan atau ditransmisikan dalam ekosistem siber. Mengingat interaksi di dunia siber tergantung pada ketersediaan, integritas, dan kerahasiaan informasi, maka perlindungan informasi dan fasilitas serta infrastruktur digital menjadi semakin penting.

Ancaman siber adalah tindakan yang mungkin muncul namun berpotensi menyebabkan masalah serius terhadap jaringan atau sistem komputer dan semua orang bisa terkena dampaknya. Dalam ranah negara misalnya, komponen yang terkomputerisasi adalah bagian dari infrastruktur penting pemerintah dan rentan terhadap peretas dan menjadi target serangan siber. Gangguan minor terhadap kinerja sistem bisa menyebabkan kerugian ekonomi yang cukup signifikan (Kovacevic & Nikolic, 2015; Tabansky, 2011). Untuk pengusaha, pencurian kekayaan intelektual serta pelanggaran keamanan dan data menjadi ancaman umum yang perlu diatasi. Sementara itu, dalam ranah individu, perlu disadari adanya risiko terkait pencurian data dan penyebaran perangkat lunak dan virus yang berbahaya (Bendovschi, 2015).

Badan Siber dan Sandi Negara (BSSN) melaporkan 290,3 juta kasus serangan siber pada 2019. Angka tersebut secara signifikan meningkat jika dibandingkan dengan 232,4 juta kasus pada tahun sebelumnya. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Pada tahun 2019, 4.586 laporan polisi diajukan melalui *Patrolisiber*, laman web Bareskrim untuk melaporkan kejahatan siber. Sebuah peningkatan dari 4.360 laporan pada 2018 (Patrolisiber, 2020). Serangan siber adalah serangan pada sistem komputer atau jaringan komputer untuk mendapatkan kendali atau akses tanpa izin ke sistem komputer yang ditargetkan (Maurer & Morgus, 2014; Marshall & Saulawa, 2015). Sementara kejahatan siber adalah aktivitas ilegal yang menggunakan dan menargetkan sistem atau jaringan komputer (ITU, 2012) untuk menimbulkan kerugian materiil atau immateriil pada pihak yang menjadi

target (Wilson, 2008). Tidak semua serangan siber didefinisikan sebagai kejahatan, tetapi baik serangan siber maupun kejahatan siber dianggap sebagai ancaman siber.

Kerugian dari serangan siber dan kejahatan siber tergantung pada karakteristik korban. Bagi korban korporasi, serangan siber dan kejahatan siber menyebabkan kerugian ekonomi dalam bentuk berkurangnya laba, kerugian nilai pasar, tuntutan hukum, dan rusaknya reputasi. Bagi korban individu, kerugian dari serangan siber dan kejahatan siber menyebabkan dampak stres dan psikologis, pencurian identitas, dan kerugian finansial (Acquisti, Friedman, & Telang, 2006; Agrafiotis et al., 2018; Telang & Watel, 2007;). Microsoft and Frost & Sullivan (2018) melaporkan bahwa pada tahun 2017 insiden keamanan siber menyebabkan kerugian ekonomi sekitar US$ 34,2 miliar di Indonesia. Penghitungan tersebut termasuk kerugian yang bersifat: langsung – kerugian finansial dari kerugian produktivitas, denda, dan biaya perbaikan; tidak langsung – hilangnya kesempatan karena perusahaan harus membangun kembali hubungan dengan konsumen setelah reputasinya rusak; dan terinduksi – insiden keamanan siber memiliki dampak pada ekonomi dan ekosistem yang lebih luas sehingga menyebabkan penurunan jumlah konsumen dan pendapatan (Microsoft & Frost & Sullivan, 2018).

Perubahan perilaku konsumen karena adanya Pembatasan Sosial Berskala Besar (PSBB) yang diberlakukan selama masa pandemi Covid-19 telah mempercepat transformasi digital Indonesia. Kementerian Komunikasi dan Informatika (Kominfo) melaporkan bahwa terdapat peningkatan 40% pengguna internet selama pemberlakuan PSBB antara Maret - April 2020 (Kominfo, 2020). Selama masa pandemi, 70% konsumen Indonesia telah mencoba setidaknya satu layanan digital, seperti belanja sembako daring atau *online*, hiburan digital, belajar secara *online*, dan perangkat lunak untuk bekerja dari rumah, seperti yang dilaporkan dalam Mobile Marketing Association (2020), sebuah asosiasi perusahaan yang membuat, menjual, dan menawarkan produk-produk digital. Peningkatan lalu lintas internet juga telah menarik pelaku-pelaku criminal siber dan berakibat pada lebih banyak lagi kasus serangan siber di Indonesia. Dari Januari hingga April 2020, ada setidaknya sekitar 88 juta kasus (BSSN, 2020), termasuk percobaan penipuan (*phising*[1]), serangan malware[2], dan pengumpulan informasi[3]. Oleh karena itu, muncul desakan untuk dibuatnya UU dan peraturan yang kuat untuk memastikan keamanan dan pengamanan dunia siber.

[1] *Phishing* adalah upaya untuk mendapatkan informasi pribadi dan sensitif seperti nama pengguna, kata sandi, atau nomor kartu kredit. Penyerang menyamar sebagai badan yang terpercaya, mengelabui korban untuk membuka email, pesan instan, atau pesan teks yang mengandung tautan berbahaya.
[2] Serangan *Malware* menyerang dengan menggunakan program atau tautan untuk mengganggu atau mendapatkan akses tidak berizin ke aktivitas harian sebuah sistem komputer. Biasanya, program *malware* telah dirancang untuk mendapatkan keuntungan finansial.
[3] Informasi yang dikumpulkan dari korban atau sistem tidak sensitif atau bersifat pribadi seperti pada percobaan *phishing*. Alih-alih, penyerang mengumpulkan informasi seperti nomor telepon, nama hewan peliharaan atau nama sekolah, yang bisa digunakan untuk menebak kata sandi atau serangan lain.

Peraturan-Peraturan untuk Keamanan Siber Indonesia

Dasar hukum untuk mengatur keamanan siber di Indonesia adalah UU Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 dan versi revisi UU ITE Nomor 19 Tahun 2016. UU ini mencakup aturan untuk beberapa pelanggaran, seperti mendistribusikan konten ilegal, pelanggaran perlindungan data, akses tidak berizin ke sistem komputer untuk mendapatkan informasi, dan sebuah pengambilalihan atau penyadapan ilegal dan tidak berizin terhadap sistem komputer atau elektronik lain. UU ITE memberikan perlindungan hukum untuk konten sistem elektronik dan transaksi elektronik. Akan tetapi, UU ini tidak mencakup aspek penting keamanan siber, seperti infrastruktur informasi dan jaringan, dan sumber daya manusia dengan keahlian di bidang keamanan siber.

Berdasarkan UU ITE tahun 2016, pemerintah mengeluarkan peraturan teknis, yaitu Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PP Nomor 71 Tahun 2019 ini mengandung pembaruan terkait penyelenggaraan keamanan siber pada sistem dan transaksi elektronik. Di samping beberapa pasal terkait pelanggaran yang diatur dalam UU ITE, PP Nomor 71 Tahun 2019 memiliki aturan lebih kuat terkait perlindungan data dan informasi pribadi, serta otentikasi laman web untuk menghindari laman web palsu atau penipuan. Selain itu, PP Nomor 71 Tahun 2019 menekankan perlunya pemerintah untuk mencegah terjadinya kerugian terhadap kepentingan masyarakat melalui penyalahgunaan informasi elektronik dan transaksi elektronik dan adanya kebutuhan untuk mengembangkan strategi keamanan siber nasional. Akan tetapi, PP Nomor 71 hanya mencakup kejahatan siber yang berhubungan dengan transaksi elektronik, seperti penyalahgunaan data, tanda tangan elektronik tidak terotorisasi, dan penyebaran virus dan tautan. Cakupan terbatas UU ITE dan PP Nomor 71 Tahun 2019 kurang merespons ancaman siber yang terus berkembang, terutama ancaman terhadap infrastruktur penting pemerintah.

Untuk menghadapi ancaman siber terhadap keamanan nasional, Peraturan Kementerian Pertahanan (Kemenhan) Nomor 82 Tahun 2014 menyediakan pedoman pertahanan siber. Peraturan itu adalah satu-satunya peraturan yang menjabarkan definisi keamanan siber: Keamanan siber nasional adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional dari serangan siber. Segala perkataan atau tindakan yang dilakukan oleh pihak manapun yang mengancam pertahanan nasional, kedaulatan, dan integritas teritorial dianggap sebagai serangan siber. Tidak seperti UU ITE, peraturan ini mencakup infrastruktur penting dari, misalnya, sistem keuangan dan transportasi sebagai objek keamanan siber. Akan tetapi, peraturan ini hanya berguna untuk mengembangkan kapasitas pertahanan siber militer, serta dikembangkan dan diimplementasikan oleh Kementerian Pertahanan dan Tentara Nasional Indonesia (TNI). Untuk ancaman siber non-militer maka akan mengacu ke peraturan lainnya, seperti UU ITE.

Upaya untuk Mengesahkan RUU Keamanan Siber

Kebijakan dan peraturan untuk keamanan siber saat ini tetap terbagi ke beberapa kementerian yang berbeda. Kurangnya payung hukum untuk keseluruhan kerangka regulasi, menyebabkan tanggung jawab tetap tidak terkoordinasi (Aprilianti & Dina, 2021; Rizal & Yani, 2016). Ada risiko situasi ini bisa menyebabkan respons pemerintah yang kurang tanggap terhadap ancaman siber yang meningkat.

Oleh karena itu, terutama dalam upaya merespons ancaman siber yang meningkat terhadap infrastruktur kritis pemerintah, Dewan Perwakilan Rakyat (DPR) dan BSSN menulis sebuah rancangan UU yang akan memayungi seluruh UU dan peraturan keamanan siber di Indonesia. Rancangan Undang-Undang Keamanan dan Ketahanan Siber ini dipelopori oleh Badan Legislasi DPR pada Mei 2019 dan seharusnya sudah disahkan menjadi UU pada September 2019. Jika sudah disahkan maka Indonesia menjadi anggota keempat ASEAN yang memiliki UU keamanan siber selain Singapura, Malaysia, dan Thailand.

Sejak Mei 2020[4], RUU Keamanan Siber memiliki 77 pasal yang mengatur masalah pelaksanaan keamanan siber, pengaturan keamanan siber, layanan keamanan siber, dan peran BSSN, diplomasi siber, dan penegakkan hukum. Jika dibandingkan dengan UU dan peraturan lain, RUU Keamanan Siber mencakup beberapa aspek keamanan siber yang krusial, seperti infrastruktur kritis, pengembangan teknologi keamanan siber di Indonesia, dan sanksi kriminal untuk yang melanggar. RUU Keamanan Siber juga bertujuan untuk mengisi kekosongan dari UU ITE terkait masalah perlindungan dan keamanan informasi dan infrastruktur jaringan, serta sumber daya manusia keamanan siber.

RUU Keamanan Siber menunjuk BSSN untuk mengkoordinasikan upaya pengembangan strategi keamanan siber dengan berkolaborasi dengan lembaga pemerintahan lainnya, seperti Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Nasional (BIN), Kepolisian Republik Indonesia, dan Tentara Nasional Indonesia (TNI). Akan tetapi, RUU tersebut tidak merinci peran antar lembaga-lembaga tersebut, dan juga tidak menjabarkan tanggung jawab BSSN dan lembaga pemerintahan lainnya dalam melindungi keamanan siber. Pasal 38 menyebutkan bahwa BSSN dapat menyaring konten dan aplikasi elektronik yang mengandung konten berbahaya guna melindungi keamanan masyarakat ketika menggunakan aplikasi elektronik. Akan tetapi, tugas menyaring konten dan aplikasi saat ini dilakukan di bawah wewenang Kominfo. Sayangnya, pasal 38 tersebut tidak mengatur koordinasi antara BSSN dan Kominfo untuk menyaring konten, dan tidak ada kriteria yang rinci terkait apa yang dianggap konten berbahaya.

Selain tidak adanya penjabaran wewenang yang jelas antara BSSN dan lembaga pemerintah terkait lainnya, asosiasi pengusaha juga mengkritik Pasal 4 dan 8 karena membatasi keterlibatan sektor swasta dan asosiasinya dalam masalah keamanan siber (Wibowo, 2019). Pasal 4 dari RUU tersebut menyatakan bahwa keamanan siber akan dilaksanakan oleh lembaga pemerintah, pemerintah pusat, pemerintah daerah, dan masyarakat. Menurut Pasal 8, masyarakat bisa terlibat dalam pelaksanaan keamanan siber ketika melindungi sistem elektronik

[4] Versi Mei 2019 tersedia di http://institute.id/wp-content/uploads/2019/09/RUU-Keamanan-dan-Ketahanan-Siber.pdf

internal perusahaan mereka atau ketika menyediakan layanan untuk keamanan siber. Namun, penggunaan kata "masyarakat" dinilai sangat luas dan mungkin tidak diinterpretasikan secara khusus untuk melibatkan semua pemangku kepentingan di sektor swasta.

Terlebih lagi, RUU ini tidak membedakan antara infrastruktur digital atau aplikasi yang membutuhkan tingkat keamanan yang berbeda-beda. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan melalui Sistem Elektronik setidaknya memperjelas perbedaan antara aplikasi pemerintah dan swasta. Sama halnya, Permenhan Nomor 82 Tahun 2014 juga telah menjabarkan objek dan infrastruktur yang perlu diamankan dalam kerangka kerja pertahanan siber. Jangankan mengembangkan tingkat keamanan yang berbeda untuk sektor publik atau swasta, bahkan perbedaannya pun tidak tertulis sama sekali dalam RUU Keamanan Siber.

Umumnya, aturan keamanan siber perlu mengenali pentingnya sektor swasta dalam membagikan dan melindungi informasi, mengembangkan metode dan operasi untuk mengendalikan teknologi, serta cara untuk mengkonfigurasi fungsi perangkat elektronik (Gallaher, Link, & Rowe, 2008). Oleh karena itu, peraturan keamanan siber sebaiknya tidak membatasi penilaian dan pemberlakuan keamanan siber itu sendiri secara umum, melainkan justru melibatkan semua pemangku kepentingan yang relevan dalam menjaga objek dan infrastruktur yang sensitif dalam keamanan siber. Peraturan keamanan siber perlu membedakan dan menjawab kebutuhan sektor publik dan swasta, mengidentifikasi tingkat keamanan siber yang dibutuhkan secara spesifik, dan mengikuti perkembangan teknologi dan ancaman-ancaman yang baru.

Oleh karena RUU Keamanan Siber saat ini masih kekurangan masukan dari badan pemerintah yang lain, pada September 2019 DPR menyatakan bahwa RUU Keamanan Siber tidak akan disahkan menjadi UU, serta diskusi RUU disebut akan dimulai kembali dari awal. Awalnya DPR telah memasukkan RUU ini dalam Program Legislasi Nasional (Prolegnas) 2020, tetapi kemudian dikeluarkan lagi (DPR, 2020). Tanpa adanya revisi yang substansial, RUU ini juga tidak dimasukkan dalam Prolegnas 2021. Alih-alih, DPR memasukkan RUU Keamanan Siber dalam daftar Prolegnas jangka menengah untuk periode legislasi 2020 – 2024.

Proses Pembuatan Kebijakan RUU Keamanan Siber yang Tertutup

Setelah diskusi RUU ini diinisiasi pada Mei 2019, naskah akademik RUU ini diunggah oleh DPR pada Juni 2019 agar bisa diakses oleh masyarakat[5]. Sementara naskah akademik dibuat tersedia untuk masyarakat, RUU Keamanan Siber itu sendiri tidak pernah diunggah ke internet. Hal tersebut memicu munculnya petisi *online*[6] yang mengkritik proses pembuatan kebijakan yang tertutup. Petisi tersebut meminta penundaan RUU Keamanan Siber dan meminta keterlibatan sektor swasta serta akademisi dalam deliberasinya. Selain itu, RUU ini juga tidak melibatkan lembaga pemerintah yang relevan, seperti Kominfo dan Badan Perencanaan Pembangunan Nasional (Aprilianti & Dina, 2021).

Proses pembuatan kebijakan yang tertutup dan dengan tidak melibatkan sektor swasta menyebabkan adanya pasal-pasal yang berpotensi menyulitkan inovasi dan pengembangan layanan dan produk keamanan siber. Pasal dalam RUU tersebut mengatur persyaratan sertifikasi untuk usaha yang merencanakan pengembangan layanan dan produk keamanan siber untuk proses pengadaan pemerintah. Namun, persyaratan ini kemungkinan menduplikasi persyaratan yang sudah ada di UU dan peraturan yang lain. Pasal 17 RUU ini juga mewajibkan pengusaha untuk mendapatkan sertifikasi BSSN untuk produk yang ingin mereka tawarkan untuk keamanan siber. Pasal 19 dan 21 mewajibkan sumber daya manusia untuk keamanan siber harus sesuai dengan standar BSSN dan mendapatkan sertifikasi dari lembaga yang terakreditasi BSSN. Namun tidak jelas apakah sertifikasi ini sama dengan yang diatur dalam UU ITE di bawah wewenang Kominfo. Jika ternyata tidak sama, maka RUU ini telah menambahkan beban kepatuhan bagi sektor swasta dan menimbulkan sistem sertifikasi yang mubazir. Kondisi tersebut secara tidak proporsional akan berdampak pada usaha kecil dan menengah yang memiliki kapasitas kepatuhan lebih rendah.

Perusahaan kecil juga akan terdampak oleh Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik yang dikeluarkan pada Desember 2020. Peraturan ini merupakan peraturan teknis seperti yang diatur dalam Pasal 24 Peraturan Pemerintah Nomor 71 Tahun 2019. Peraturan BSSN Nomor 8 Tahun 2020 menjelaskan perlunya penyelenggara sistem elektronik (publik dan swasta) untuk memastikan keamanan pengelolaan informasi mereka. Peraturan-peraturan ini mewajibkan penyelenggara sistem elektronik untuk menggunakan seorang ahli keamanan (lokal atau asing) atau konsultan untuk mengawasi pelaksanaan sistem elektronik mereka. Akan tetapi, tidak ada penjelasan mengenai kebutuhan kualifikasi para ahli atau konsultan tersebut sesuai dengan standar BSSN. RUU Keamanan Siber pun mengikuti persyaratan yang sama dan tidak mengelaborasi keahlian yang disyaratkan.

Selain dari sertifikasi produk, Pasal 48 RUU Keamanan Siber menunjuk BSSN untuk mengeluarkan izin penelitian terhadap aplikasi keamanan siber, atau mengujinya. Hal ini semakin menambah kebingungan, karena pasal tersebut tidak menentukan kegiatan penelitian atau pengujian keamanan siber seperti apa yang membutuhkan izin dari BSSN.

Terakhir, pasal 66 RUU Keamanan Siber mewajibkan para pengusaha untuk memenuhi persyaratan kandungan lokal, yaitu 50% Tingkat Komponen Dalam Negeri (TKDN). Mengingat kebanyakan pengusaha menggunakan perangkat keras dan lunak dari luar negeri untuk produk dan jasa mereka, maka persyaratan 50% TKDN akan berdampak pada pengembangan produk dan jasa keamanan siber di Indonesia.

[5] Tulisan akademik RUU Keamanan Siber dapat diakses di http://dpr.go.id/doksileg/proses1/RJ1-20190617-025848-5506.pdf.
[6] Petisi tersebut bisa diakses di https://www.change.org/p/dewan-perwakilan-rakyat-tolak-ruu-kks-ruu-kks-bermasalah

Semua pasal yang disebutkan seakan berlawanan dengan tujuan untuk meningkatkan persaingan dan inovasi siber melalui penggunaan siber yang bebas, terbuka, dan bertanggung jawab seperti yang tercantum pada Pasal 3 (b) RUU Keamanan Siber. Tujuan tersebut hanya bisa dicapai dalam sebuah dialog yang sarat makna dengan pemangku kepentingan yang relevan dari sektor pengusaha, akademisi, dan masyarakat.

Selain itu, transparansi adalah salah satu prinsip yang ditetapkan oleh UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan di Indonesia. Hal tersebut dimanifestasikan dengan membagi rancangan UU ke publik untuk mendapatkan masukan dari publik dan pemangku kepentingan yang terkait. Selain itu, publik juga memiliki hak untuk memberikan masukan secara lisan maupun tulisan selama proses legislasi. UU tersebut juga mengatur beberapa cara bagi masyarakat untuk memberikan masukan, termasuk rapat dengar pendapat, kunjungan kerja, sosialisasi, seminar, lokakarya, dan diskusi. Itulah sebabnya proses pembuatan kebijakan RUU Keamanan Siber yang tertutup dikritik karena tidak mengindahkan UU ini.

Rekomendasi Kebijakan

Melibatkan pemangku kepentingan terkait dalam proses pembuatan kebijakan adalah sebuah langkah yang penting. Pemerintah bisa memilih untuk menggunakan pendekatan *multi-stakeholder* melalui Dialog Pemerintah – Swasta atau *Public-Private Dialogue* (PPD) untuk membahas isu kebijakan yang problematik dan menantang (Shear, Schnidrig, & Kaspar, 2018). Pemerintah yang menggunakan pendekatan PPD telah terbukti bisa membuat reformasi yang tepat sasaran dan bisa diimplementasikan. Secara bersamaan, sektor swasta yang terlibat dalam PPD cenderung akan lebih mendukung pelaksanaan kebijakan itu sendiri (Bannock, 2005; Herzberg & Wright, 2005).

Dalam keamanan siber, sektor swasta bukan hanya menjadi korban serangan siber namun juga merupakan pihak yang harus merespons. Banyak perusahaan telah mengembangkan solusi sebagai upaya mitigasi serangan siber dan hal itu bisa menguntungkan masyarakat mengingat selama pandemi Covid-19 komputer pribadi dan perangkat lunak yang digunakan untuk bekerja dan belajar dari rumah telah terkena serangan siber (Bahsi & Karabacak, 2020). Selain itu, perusahaan-perusahaan teknologi juga telah beradaptasi dengan situasi baru ini dengan meningkatkan keamanan produk dan jasa mereka. Perusahaan yang menawarkan layanan berbasis komputasi awan (*cloud-based*) telah meningkatkan keamanan mereka untuk meyakinkan konsumen bahwa data mereka aman. Perusahaan yang menawarkan perangkat lunak konferensi-video secara berkelanjutan juga memperbarui produk mereka dengan peningkatan keamanan dan privasi.

Keamanan siber adalah isu penting dan berdampak tidak hanya pada pemerintah, namun juga pada sektor swasta dan masyarakat. Keahlian sektor swasta bisa memberikan informasi kepada pemerintah tentang teknologi keamanan siber terbaru dan kemudian juga memperkuat pertukaran informasi/pengetahuan antara pemerintah dan sektor swasta. Kondisi tersebut akan menguntungkan pemerintah selama masa pembuatan dan pelaksanaan kebijakan keamanan siber. Mengabaikan sektor swasta akan berakibat pada respons yang tidak cukup untuk menjaga keamanan siber (Llorente, 2018).

Dialog antara pemerintah dan sektor swasta harus fokus pada pengembangan sebuah kerangka kerja keamanan siber nasional. Membuat platform *online* untuk mengumpulkan masukan merupakan hal yang praktis, terutama saat masa pandemi seperti sekarang. Kerangka kerja ini penting untuk menjadi payung bagi peraturan yang sudah ada dan diharapkan bisa menginspirasi DPR dan BSSN untuk fokus pada peningkatan RUU Keamanan Siber.

Selain itu, RUU Keamanan Siber perlu dengan jelas mendefinisikan keamanan siber dan menjabarkan peran, tanggung jawab, dan wewenang lembaga pemerintah terkait. Hal itu akan mengizinkan BSSN untuk mengkoordinasikan semua upaya keamanan siber seluruh lembaga pemerintah terkait.

Referensi

Acquisti, A., Telang, R., & Friedman A. (2006). Is there a cost to privacy breaches? An event study. *Proceedings of the 3rd International Conferences on Intelligent System*.

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding hot they propagate. *Journal of Cybersecurity*. Doi: 10.1093/cybsec/tyy006

Aprilianti, I., & Dina, S. (2021). Pengaturan Bersama Ekonomi Digital Indonesia. *Center for Indonesian Policy Studies*. Diambil dari: https://repository.cips-indonesia.org/publications/332998/co-regulating-the-indonesian-digital-economy

Badan Siber dan Sandi Negara. (2020). Rekap Serangan Siber (Januari – April 2020). Diambil dari: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Badan Siber dan Sandi Negara. (2020). Indonesia cyber security monitoring report 2019. Diambil dari: https://bssn.go.id/laporan-tahunan-2019-pusopkamsinas-bssn/

Bahsi, H., & Karabacak, B. (2020). Covid-19 pandemic crisis and its implication on Cybersecurity. *Information Security Journal: A Global Perspective*. Diambil dari: https://think.taylorandfrancis.com/special_issues/covid-19-cybersecurity/#?utm_source=CPB&utm_medium=cms&utm_campaign=JPG15743%20

Bannock Consulting Ltd. (2005). Reforming the business enabling environment, mechanism, and processes for Private-Public Sector Dialogue. Diambil dari: http://ppd.cipe.org/global-workshops/workshop-2006/reforming-the-business-enabling-environment-mechanisms- and-processes-for-private-public-sector-dialogue/.

Bendovschi, A. (2015). Cyber-attacks – trends, patterns, and security countermeasures. *Procedia Economics and Finance*. Doi: 10.1016/S2212-5671(15)01077-1

Dewan Perwakilan Rakyat. (2020). Program Legislasi Nasional Prioritas. Diambil dari: https://www.dpr.go.id/uu/prolegnas

Frost & Sullivan. (2018). Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar. Diambil dari: https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi- di-indonesia-sebesar-us34-2-miliar/

Gallaher, M., Link, A., & Rowe, B. (2008). Cyber security: Economic strategies and public policy alternative. Cheltenham, England: Edward Elgar Publishing.

Herzberg, B., & Wright, A. (2005). Competitiveness partnership: Building and Mantaining Public-Private Dialogue to Improve the Investment Climate. A resource drawn from 40 countries experience. *International Finance Corporation (IFC)*.

Internet Development Institute. (2019). Tolak RUU KKS! RUU KKS Bermasalah! *Change.org*. Diambil dari:https://www.change.org/p/dewan-perwakilan-rakyat-tolak-ruu-kks-ruu-kks-bermasalahIndonesia Criminal Investigation Agency. (2020). Statistik jumlah Laporan Polisi yang dibuat masyarakat. Diambil dari: https://patrolisiber.id/statistic

International Telecommunication Union. (2012). Understanding cybercrime: phenomena, challenges, and legal response. Diambil dari: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Kementerian Komunikasi dan Informatika. (2020). Penggunaan Internet Naik 40% Saat Bekerja dan Belajar dari Rumah. Diambil dari: https://www.kominfo.go.id/content/detail/25881/penggunaan-internet-naik-40-saat-bekerja-dan-belajar-dari-rumah/0/berita_satker

Kovacevic, A., & Nikolic, D. (2015). Cyber-attacks on critical infrastructure: Review and challenges. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance.* Doi: 10.4018/978-1-4666-6324-4.ch001

Llorente, R. (2018). A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity. *LSE IDEAS*. Diambil dari: https://lseideas.medium.com/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622

Marshall, J., & Saulawa, M. (2015). Cyberattack: the legal response. *International Journal of International Law*, 1 (2). Diambil dari: http://www.ijoil.com/wp-content/uploads/2015/04/CYBER-ATTACKS-ACCEPTED-JOURNAL-1.pdf.

Maurer, T., & Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. *New America Research Report.*

Mobile Marketing Association. (2020). Impact of Covid-19 on Consumer Behaviour in Indonesia. Diambil dari: https://www.mmaglobal.com/indonesia/node/34611

Rizal, M., & Yani, Y. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, 4 (1).

Setiadi, F., Sucahyo, Y., & Hasuban, Z. (2012). An overview of the development Indonesia's national cybersecurity. *International Journal of Information Technology & Computer Science*, 6.

Shears, M., Schnidrig, D., & Kaspar, L. (2018). Multistakeholder Approaches to National Cybersecurity Strategy Development. *Global Partners Digital.* Diambil dari:https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

Tabansky, L. (2011). Critical infrastructure protection against cyber threats. *Military and Strategic Affairs*, 3 (2). Diambil dari: https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf.

Telang, R., & Wattal S. (2007). An empirical analysis of the impact of software vulnerability announcement on firm stock price. *IEEE Transactions on Software Engineering*, 33. Doi: 10.1109/TSE.2007.70712

Wibowo, S. (2019). Membongkar borok RUU Keamanan dan Ketahanan Siber. *CNNIndonesia*. Diambil dari https://www.cnnindonesia.com/teknologi/20190905204826-186-427990/membongkar-borok-ruu-keamanan-dan-ketahanan-siber

Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress. *Congressional Research Service*.

TENTANG PENULIS

Noor Halimah Anjani adalah Peneliti Muda di CIPS dengan spesialisasi pada isu pertanian serta ekonomi digital. Sebelum bergabung dengan CIPS, Halimah bekerja sebagai asisten peneliti di Universitas Katolik Parahyangan untuk topik kajian pekerja migran perempuan dan penggunaan remitansi untuk penanggulangan kemiskinan. Ia juga telah mempublikasikan artikel mengenai isu internasional terkait *Belt and Road Initiative* dari Pemerintah Republik Rakyat Tiongkok.

Halimah lulus dari Universitas Katolik Parahyangan dengan gelar Sarjana Hubungan Internasional dan dia adalah salah satu alumni CIPS Emerging Policy Leaders Program (EPLP) 2020.

CIPS
Center for Indonesian Policy Studies

Center for Indonesian Policy Studies (CIPS) merupakan lembaga pemikir non-partisan dan non profit yang bertujuan untuk menyediakan analisis kebijakan dan rekomendasi kebijakan praktis bagi pembuat kebijakan yang ada di dalam lembaga pemerintah eksekutif dan legislatif.

CIPS mendorong reformasi sosial ekonomi berdasarkan kepercayaan bahwa hanya keterbukaan sipil, politik, dan ekonomi yang bisa membuat Indonesia menjadi sejahtera.

Center for Indonesian Policy Studies

contact@cips-indonesia.org

Jalan Terogong Raya No. 6B Cilandak,
Jakarta Selatan 12430, Indonesia

www.cips-indonesia.org

Kerja kami bergantung pada dukungan Anda. Kunjungi **www.cips-indonesia.org/donate** untuk mendukung CIPS.