CIPS
Center for Indonesian Policy Studies

idEA
Asosiasi E-Commerce Indonesia

Makalah Kebijakan No. 39

Kajian Pemenuhan Akses Terhadap Data dan Sistem dari Penyelenggara Sistem Elektronik oleh Kementerian, Lembaga Pengawas, dan Aparat Penegak Hukum

oleh Ajisatria Suleiman

www.cips-indonesia.org

Makalah Kebijakan No. 39

Kajian Pemenuhan Akses Terhadap Data dan Sistem dari Penyelenggara Sistem Elektronik oleh Kementerian, Lembaga Pengawas, dan Aparat Penegak Hukum

Penulis:
Ajisatria Suleiman
Center for Indonesian Policy Studies (CIPS)

Ucapan Terima Kasih:
Makalah ini didukung oleh Asosiasi E-Commerce Indonesia, yang menghormati independensi analisis kami. Untuk menjaga integritas akademik dan non-keberpihakan institusional kami secara ketat, CIPS secara eksklusif bekerja sama dengan donor yang tidak menentukan arah temuan, kesimpulan, atau rekomendasi yang disajikan dalam publikasi kami.

Sampul:
freepik.com/onlyyouqj

Jakarta, Indonesia
September, 2021

DAFTAR ISI

Daftar Tabel

GLOSARIUM

PSE:
Penyelenggara Sistem Elektronik.

APH:
Aparat Penegak Hukum.

Permen 5:
Peraturan Menteri Komunikasi dan Informatika No. 5/2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat.

Dwang middelen:
Upaya Paksa.

SMPI:
Sistem Manajemen Pengamanan Informasi.

Kominfo:
Kementerian Komunikasi dan Informatika.

K/L:
Kementerian/Lembaga.

RINGKASAN EKSEKUTIF

Kewenangan dari instansi negara untuk mengakses data elektronik milik *platform* atau Penyelenggara Sistem Elektronik swasta merupakan topik yang cukup banyak diperbincangkan oleh pakar internasional karena beragamnya praktik negara-negara di dunia. Indonesia menjadi salah satu negara yang merumuskan ketentuan ini dalam Peraturan Menteri Komunikasi dan Informatika No. 5/2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat ("**Permen 5**"). Berkaca dari berbagai pandangan akademisi internasional dan pengalaman di negara lain seperti Amerika Serikat, Korea Selatan, Brazil, India, dan Tiongkok kajian ini memberikan masukan untuk menyempurnakan materi muatan Permen 5. Dari aspek legalitas, diperlukan landasan hukum yang lebih kuat untuk memastikan partisipasi politik publik, serta kebutuhan mekanisme pengujian dan keberatan oleh badan independen. Selain itu, idealnya UU tentang Perlindungan Data Pribadi sah dan berlaku sebelum kewenangan akses oleh instansi negara dapat berjalan dengan baik. Dalam situasi saat ini, Kementerian Kominfo perlu berperan sebagai pembina dan pelindung (atau *privacy safeguard*) untuk memastikan akses oleh kementerian dan lembaga untuk kepentingan pengawasan sudah sesuai dengan prinsip perlindungan data pribadi. Kajian ini juga menyimpulkan bahwa akses terhadap sistem PSE bukan merupakan *best practice*, sehingga sebaiknya dijadikan alternatif terakhir dan semua langkah mitigasi risiko keamanan informasi sudah dijalankan.

PENDAHULUAN

Peraturan Menteri Komunikasi dan Informatika No. 5/2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat ("**Permen 5**") yang akan berlaku pada pertengahan Mei 2021 membawa perubahan yang signifikan terhadap tata kelola akses data dan sistem dari PSE oleh lembaga pemerintah, atau regulator, dan aparat penegak hukum (APH). Pasal 21 Permen 5 menyatakan bahwa PSE Lingkup Privat wajib memberikan akses terhadap Sistem Elektronik dan/atau Data Elektronik kepada, (a) kementerian atau lembaga dalam rangka pengawasan sesuai dengan peraturan perundang-undangan, dan (b) APH dalam rangka penegakan hukum sesuai dengan peraturan perundang-undangan.

Selanjutnya dalam Pasal 3 ayat (4) butir (i), disebutkan bahwa setiap PSE Lingkup Privat wajib melampirkan di dalam dokumen pendaftaran wajibnya, surat keterangan yang menyatakan bahwa PSE Lingkup Privat menjamin dan melaksanakan kewajiban pemberian akses terhadap Sistem Elektronik dan Data Elektronik dalam rangka memastikan efektivitas pengawasan dan penegakan hukum sesuai dengan ketentuan peraturan perundang-undangan.

Di satu sisi, ketentuan mengenai tata kelola akses data dan sistem dalam Permen 5 dapat menjadi pedoman dan rujukan standar dari kementerian/lembaga (K/L) maupun APH untuk dapat menjalankan kewenangan mereka dan meminta akses terhadap data dan sistem dari Penyelenggara Sistem Elektronik. Dalam hal ini Kementerian Komunikasi dan Informatika, atau Kominfo, dapat menjadi pembina dan pembimbing agar memastikan kewenangan dari K/L dan APH dapat dijalankan dengan memperhatikan perlindungan data pribadi dan prosedur yang adil (*due process*).

> "Akses terhadap data dan sistem dari PSE merupakan isu yang sensitif karena menyangkut upaya paksa (*dwang middelen*) yang dapat berdampak bagi perlindungan Hak Asasi Manusia dan kemerdekaan individu, serta berkaitan erat dengan perlindungan data pribadi maupun rahasia dagang milik PSE (termasuk hak-hak kekayaan intelektual yang terkait seperti hak cipta)."

Namun di sisi lain, akses terhadap data dan sistem dari PSE merupakan isu yang sensitif karena menyangkut upaya paksa (*dwang middelen*) yang dapat berdampak bagi perlindungan Hak Asasi Manusia dan kemerdekaan individu, serta berkaitan erat dengan perlindungan data pribadi maupun rahasia dagang milik PSE (termasuk hak-hak kekayaan intelektual yang terkait seperti hak cipta). Apabila tidak dijalankan dengan hati-hati akses terhadap sistem juga berpotensi membuka celah keamanan yang dapat mengganggu postur sistem keamanan informasi dari PSE. Hal-hal ini merupakan permasalahan kepentingan publik yang perlu dijaga dan dilindungi.

Permen 5 sebenarnya sudah membahas hal-hal mendasar ini. Misalnya, terkait dengan akses terhadap data, diperlukan penilaian (*assessment*) atas kepentingan pengawasan dan proporsionalitas serta legalitas, dan juga perlu disebutkan secara eksplisit ruang lingkup atau jenis sistem atau data elektronik yang hendak diakses. Akses juga hanya dapat digunakan untuk kepentingan yang disebutkan dalam permintaan. Khusus pemberian akses, dalam Pasal 30 juga disebutkan bahwa ada komponen-komponen yang perlu dilindungi yaitu, integritas, ketersediaan, dan kerahasiaan dari Data Elektronik; keandalan dan keamanan Sistem Elektronik; serta Data Pribadi yang terkait.

Namun demikian, tetap perlu dilakukan kajian yang lebih mendalam untuk menilai apakah Permen 5 sudah mengakomodasi berbagai elemen-elemen kunci yang dapat menjaga dan memastikan (atau istilahnya *safeguard*) terlindunginya prinsip-prinsip umum HAM, hak kekayaan intelektual, dan perlindungan data pribadi.

Pembahasan topik ini pun tidak eksklusif di Indonesia, mengingat perdebatan yang mirip berlangsung juga di negara-negara lain di dunia. Di Amerika Serikat, contohnya, terdapat perdebatan mengenai definisi "meta-data" dan "data", dimana akses terhadap meta-data cukup menggunakan surat perintah (*subpoena*), sementara akses terhadap data perlu membutuhkan surat perintah penyitaan (*court order*) dari pengadilan (Nissenbaum et al., n.d.). Perdebatan lain misalnya terkait dengan kepentingan keamanan nasional, dimana proses akses data untuk kepentingan yang membahayakan keamanan seperti terorisme dapat melalui dokumentasi yang lebih sederhana (Rubinstein et al., 2014).

Di tengah perdebatan yang timbul ini, pengalaman dari negara lain dapat menjadi acuan untuk menilai legitimasi dan kelayakan Permen 5. Negara seperti Amerika Serikat, Brazil, Korea Selatan, Tiongkok, dan India semua memiliki pengaturan mengenai akses Pemerintah terhadap data. Dengan pengecualian proyek *Golden Shield* di Tiongkok, semua negara-negara ini memiliki legislasi khusus yang dibahas melalui suatu proses politik di parlemen yang merupakan representasi suara masyarakat dalam proses pengambilan kebijakan. Referensi dan literatur dari negara-negara ini juga menunjukan bahwa akses Pemerintah umumnya ditujukan pada data elektronik, bukan sistem elektronik.

Berlandaskan latar belakang ini, penelitian ini akan menjawab pertanyaan-pertanyaan ini:

a. Apa saja prinsip umum yang perlu dijadikan pedoman dalam melakukan akses data dan sistem pada pelaku usaha digital?
b. Apakah Permen 5 sudah mengadopsi prinsip-prinsip umum yang ada?
c. Apa saja pelajaran yang dapat diambil dari praktik di negara-negara lain?
d. Bagaimana seharusnya pelaku usaha dapat bersikap di tengah perdebatan yang ada?
e. Apa kebijakan yang diperlukan bagi Indonesia di masa mendatang?

PRINSIP-PRINSIP DASAR DAN KEPENTINGAN UMUM

> Perusahaan teknologi seharusnya berhak dan wajib memiliki prosedur untuk menilai dengan hati-hati tidak hanya apakah permintaan pemerintah itu sah, tetapi juga apakah itu sudah atau tidak sesuai dengan standar HAM internasional.

Keabsahan kewenangan dari suatu instansi pemerintah untuk mengakses data milik *platform* atau PSE swasta sudah cukup banyak diperbincangkan oleh para pakar. Pedoman implementasi *Global Network Initiative* (GNI)[1] menyatakan bahwa tidak cukup bagi suatu perusahaan teknologi mengatakan, "kami hanya mengikuti aturan yang ada (Global Network Initiative, 2018)." Perusahaan teknologi seharusnya berhak dan wajib memiliki prosedur untuk menilai dengan hati-hati tidak hanya apakah permintaan pemerintah itu sah, tetapi juga apakah itu sudah atau tidak sesuai dengan standar HAM internasional. Pedoman GNI menyatakan bahwa, jika diminta untuk memberikan informasi pribadi kepada otoritas pemerintah, setiap perusahaan sewajarnya berhak dan wajib:

1. Menafsirkan dan menerapkan secara terbatas tuntutan pemerintah yang dianggap melanggar perlindungan data pribadi
2. Meminta klarifikasi atau modifikasi dari otoritas yang berwenang ketika tuntutan pemerintah tampak berlebihan, melanggar hukum, tidak diwajibkan oleh hukum yang berlaku atau tidak sejalan dengan hukum dan standar hak asasi manusia internasional tentang privasi.
3. Meminta komunikasi yang jelas, sebaiknya secara tertulis, yang menjelaskan dasar hukum permintaan pemerintah atas informasi pribadi, termasuk nama badan pemerintah yang meminta dan nama, jabatan, dan tanda tangan pejabat yang berwenang.
4. Mengharuskan pemerintah mengikuti proses hukum domestik yang ditetapkan saat mereka mencari akses ke data pribadi.
5. Mengadopsi kebijakan dan prosedur untuk menangani bagaimana perusahaan akan menanggapi ketika tuntutan pemerintah tidak menyertakan arahan tertulis atau tidak mampu untuk mematuhi prosedur hukum yang ditetapkan. Kebijakan dan prosedur ini harus mencakup pertimbangan mengapa berkeberatan atas permintaan pemerintah tersebut.
6. Menafsirkan secara terbatas kewenangan otoritas pemerintah untuk mengakses data pribadi,
7. Mengajukan keberatan kepada pemerintah di pengadilan domestik atau mencari asistensi dari otoritas terkait, lembaga HAM internasional atau organisasi non-pemerintah ketika dihadapkan pada permintaan pemerintah yang tampaknya tidak sesuai dengan hukum atau prosedur domestik atau hukum dan standar HAM internasional tentang perlindungan data pribadi (Global Network Initiative, 2018, pp. 8–9).

[1] The Global Network Initiative adalah kolaborasi multi-stakeholder collaboration dari perusahaan, aktivis HAM, investor, dan pemangku kepentingan lain untuk memastikan perusahaan teknologi tunduk terhadap prinsip-prinsip HAM, perlindungan data pribadi, dan kebebasan berekspresi, khususnya terkait akses data, dan pemblokiran konten. Lihat https://www.globalnetworkinitiative.org/.

Nico van Eijk, Guru Besar bidang *Media and Telecommunications Law* dan Direktur *Institute for Information Law* (IViR, Faculty of Law, University of Amsterdam) mengidentifikasi 7 prinsip umum untuk memastikan adanya pengawasan serta *check-and-balances* atas akses data oleh Pemerintah sebagai berikut (van Eijk, 2017):

1. Perlu ada pengawasan yang komprehensif, dalam tiga hal: (a) pemerintah (cabang eksekutif), legislatif, yudikatif, dan komisi khusus (non-parlementer, independen) harus semuanya berperan, (b) Pengawasan harus mencakup pra-pengawasan, pengawasan berkelanjutan, dan pengawasan setelah fakta, dan (c) Mandat badan pengawas harus mencakup tinjauan atas keabsahan dan keefektifan permintaan akses.
2. Perlu ada pengawasan yang mencakup semua tahapan siklus data, termasuk pengumpulan, penyimpanan, kueri, dan analisis data.
3. Perlu ada badan pengawas yang independen dari badan intelijen dan pemerintah, seperti mekanisme peradilan yang independen.
4. Pengawasan dapat dilakukan sebelum penerapan akses (pra-tindakan) ataupun kombinasi dengan pengawasan pasca-tindakan melalui sebuah komisi khusus yang independen; adanya fungsi pengawasan oleh komite parlemen; dan kemungkinan individu untuk mengajukan keberatan di hadapan badan independen
5. Badan pengawas harus dapat menyatakan tindakan yang melanggar hukum dan memberikan ganti rugi.
6. Pengawasan harus memastikan adanya kesempatan bagi pelapor dan terlapor untuk saling sanggah (adversarial).
7. Badan pengawas harus memiliki sumber daya yang cukup untuk bekerja secara efektif.

Akademisi terpandang lain, Jennifer Daskal, Professor dan Direktur *Tech, Law, Security Program* dari American University Washington College of Law serta Andrew K. Woods dari University of Arizona College of Law mengusulkan suatu prinsip-prinsip umum untuk memastikan kesetaraan perlindungan hukum atas akses terhadap data (Daskal & Woods, 2015). Prinsip-prinsip ini dapat dijadikan pedoman sebagai berikut:

1. **Otorisasi Independen**. Dibutuhkan lembaga yang independen untuk memastikan bahwa permintaan akses sudah didasari oleh sebab/kausa yang tepat, sudah sesuai dengan kewenangan lembaga tersebut berdasarkan ketentuan peraturan perundang-undangan yang ada, dan sudah sesuai dari segi proporsionalitasnya. Lembaga independen yang dimaksud umumnya adalah badan peradilan, yang umumnya mengeluarkan semacam surat perintah pengadilan. Kehadiran lembaga pengadilan juga dapat menjadi lembaga yang dapat dijadikan sarana keluhan atau keberatan seandainya PSE atau individu yang bersangkutan merasa keberatan dengan permintaan akses.
2. **Sebab / Kausa**. Adanya alasan atau penyebab faktual yang kuat atas permintaan akses, misalnya telah terjadi suatu kejahatan atau dalam rangka pengawasan kegiatan tertentu. Prinsip ini untuk mencegah *abuse of power* dari pihak yang meminta akses bukan untuk kepentingan jabatannya.
3. **Cakupan Spesifik**. Permintaan akses perlu spesifik merujuk pada orang tertentu,

akun tertentu, atau perangkat tertentu, serta juga menjabarkan tipe, jangka waktu, dan cakupan data yang dibutuhkan. Prinsip ini juga untuk mencegah *abuse of power* dari pihak yang meminta akses bukan untuk kepentingan jabatannya.

4. **Legalitas**. Setiap permintaan akses harus berdasarkan hukum dan kewenangan dalam peraturan perundang-undangan. Dasar, basis, atau pertimbangan hukum ini perlu disebutkan secara spesifik dalam setiap permintaan akses.
5. **Proporsionalitas**. Setiap negara perlu mengatur tindakan-tindakan apa saja yang dapat memicu permintaan akses. Misalnya untuk kepentingan penegakan hukum, hanya tindak pidana dengan ancaman tertentu saja yang dapat memicu hak akses.
6. **Pemberitahuan ke pengguna/pemilik atau subyek data**. Selaras dengan prinsip perlindungan data pribadi, perlu ada itikad baik dan tindakan yang wajar untuk memberitahukan permohonan akses kepada subyek data. Dalam hal tertentu, misalnya dalam proses penyidikan tindak pidana, pemberitahuan dapat diundur hingga masuk ke tahap tertentu. Namun tetap pada akhirnya kewajiban ini perlu dilaksanakan oleh pihak yang meminta akses atas data.
7. **Jaminan Kebebasan Berekspresi**. Permintaan akses terhadap data atau sistem tidak boleh dijadikan instrumen represif untuk menekan warga negara yang hendak menjalankan haknya untuk berekspresi dan menyampaikan pendapat.
8. **Minimisasi pengumpulan data**. Dalam rangka menjaga kepentingan perlindungan data pribadi, pengumpulan data pribadi perlu dibatasi hanya untuk data pribadi yang berkaitan dengan sebab/kausa.
9. **Pengecualian dalam keadaan darurat**. Daskal dan Woods (2015) juga menyadari bahwa proses dan prosedur permintaan akses dapat dikecualikan atau disederhanakan dalam keadaan darurat. Oleh karena itu, perlu diatur hal-hal apa saja yang tergolong sebagai keadaan darurat, misalnya dalam kejadian yang berpotensi mengancam keselamatan atau nyawa seseorang (*life threatening situation*).
10. **Transparansi**. Kementerian, lembaga, atau APH wajib menjunjung tinggi transparansi atas permintaan akses. Perlu ada suatu mekanisme misalnya dalam bentuk laporan tahunan berkala dari APH atau K/L, atau bentuk audit lainnya, yang menunjukan jumlah permintaan akses, termasuk tipe permintaan dan cakupan akses, berikut dengan informasi lain yang dipandang perlu.

MATERI MUATAN PERMEN KOMINFO 5 DAN PERMASALAHANNYA

Permen 5 mengatur masing-masing dua (2) subyek dan dua (2) obyek yang menjadi materi muatan pengaturan.

Dari segi subyek, Permen 5 memberikan kewenangan bagi Kementerian/Lembaga (didefinisikan sebagai "Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya"), dan Aparat Penegak Hukum atau APH.

Dari segi obyek yang dapat diakses, Permen 5 mengatur mengenai akses terhadap "data elektronik" dan akses terhadap "sistem elektronik." Dalam Permen ini dijabarkan bahwa, "Data Elektronik" adalah "data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi." Sementara, "Sistem Elektronik" adalah "serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik." Perbedaan tingkat risiko akses terhadap data dan terhadap sistem sudah dijabarkan di dalam bab sebelumnya.

Atas dasar ini, diberikan matriks perbandingan antara dua subyek dan dua obyek dari Permen 5, agar dapat dilakukan analisis yang lebih mendalam sebagai berikut:

Tabel 1.
Matriks Perbandingan antara Dua Subyek dan Dua Obyek dari Permen 5

	Kementerian/Lembaga	Aparat Penegak Hukum atau APH
Data	**Persyaratan yang perlu disampaikan** a. dasar kewenangan Kementerian atau Lembaga; b. maksud dan tujuan serta kepentingan permintaan; dan c. deskripsi secara spesifik jenis Data Elektronik yang diminta **Deadline**: 5 hari **Metode**: link atau cara lain, dalam jangka waktu tertentu	**Persyaratan yang perlu disampaikan** a. dasar kewenangan Aparat Penegak Hukum; b. maksud dan tujuan serta kepentingan permintaan; c. deskripsi secara spesifik jenis Data Elektronik yang diminta; d. tindak pidana yang sedang disidik, dituntut, atau disidangkan. e. Syarat tambahan khusus konten komunikasi: ***surat penetapan dari ketua pengadilan negeri dalam wilayah mana Institusi Penegak Hukum tersebut memiliki kewenangan.*** **Cakupan**: khusus pidana ancaman min. 2 tahun, dan data terkait WNI atau badan hukum Indonesia **Deadline**: 5 hari **Metode**: link atau cara lain, dalam jangka waktu tertentu
Sistem	**Persyaratan yang perlu disampaikan** a. dasar kewenangan Kementerian atau Lembaga;	Persyaratan yang perlu disampaikan a. dasar kewenangan Aparat Penegak Hukum; b. maksud dan tujuan serta kepentingan permintaan;

	b. maksud dan tujuan serta kepentingan permintaan; c. deskripsi secara spesifik Sistem Elektronik yang diminta; d. pejabat dari Kementerian atau Lembaga yang akan mengakses Sistem Elektronik yang diminta. **Deadline**: 5 hari **Metode**: pemberian hasil pemeriksaan atau audit atas Sistem Elektronik yang ruang lingkup pemeriksaan atau auditnya diminta oleh Kementerian atau Lembaga	c. deskripsi secara spesifik Sistem Elektronik yang diminta; d. tindak pidana yang sedang disidik, dituntut, atau disidangkan; e. Aparat Penegak Hukum yang akan mengakses Sistem Elektronik yang diminta; f. ***surat penetapan dari ketua pengadilan negeri dalam wilayah mana Institusi Penegak Hukum tersebut memiliki kewenangan*** **Cakupan**: khusus pidana ancaman min. 5 tahun, atau 2-5 tahun, dan hanya data terkait WNI atau badan hukum Indonesia **Deadline**: 5 hari **Metode**: pemberian hasil pemeriksaan atau audit atas Sistem Elektronik yang ruang lingkup pemeriksaan atau auditnya diminta oleh Kementerian atau Lembaga

Sumber: Peraturan Menteri Komunikasi dan Informatika No.5/2020, diolah oleh penulis.

Dari persandingan yang dilakukan, terdapat beberapa permasalahan dari Permen 5 sebagai berikut.

Akses terhadap data *vis-à-vis* penyitaan. Akses terhadap data dapat dianalogikan suatu bentuk penyitaan dari barang, dimana dalam hal ini barang tersebut merupakan data elektronik. Dengan analogi ini, dapat dikaji pengaturan mengenai penyitaan dalam Kitab Undang-Undang Hukum Acara Pidana ("KUHAP"), yaitu dalam Pasal 1 angka 16 KUHAP, Pasal 38 s/d 46 KUHAP, Pasal 82 ayat (1) dan ayat (3) KUHAP dalam konteks Praperadilan, Pasal 128 s/d 130 KUHAP, Pasal 194 KUHAP, dan Pasal 215 KUHAP. Definisi dari Penyitaan telah dirumuskan dalam P**asal 1 angka 16 KUHAP**, yaitu: "*penyitaan adalah serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan*."

Oleh karena Penyitaan termasuk dalam salah satu upaya paksa (*dwang middelen*) yang dapat melanggar Hak Asasi Manusia, maka sesuai ketentuan Pasal 38 KUHAP, Penyitaan hanya dapat dilakukan oleh penyidik dengan izin dari Ketua Pengadilan Negeri setempat, namun dalam keadaan mendesak, Penyitaan tersebut dapat dilakukan penyidik lebih dahulu dan kemudian setelah itu wajib segera dilaporkan ke Ketua Pengadilan Negeri, untuk memperoleh persetujuan.

Pengaturan internal Kepolisian Republik Indonesia mengatur bahwa dalam keadaan yang sangat perlu dan mendesak, penyitaan dapat dilakukan tanpa Surat Izin Ketua Pengadilan Negeri, dan tidak diperlukan Surat Perintah Penyitaan. Namun penyitaan ini terbatas hanya terdapat benda bergerak saja. Selanjutnya dalam hal tertangkap tangan, juga tidak diperlukan Surat izin/Surat Izin Khusus Ketua Pengadilan Negeri dan tidak diperlukan Surat Perintah Penyitaan. Namun penyitaan ini dapat hanya dilakukan terhadap benda dan alat yang ternyata diduga telah dipergunakan untuk melakukan tindak pidana atau benda lain yang dapat dipakai sebagai barang bukti.

Dengan analogi ini, terlihat bahwa ada perbedaan antara akses terhadap sistem *vis-à-vis* penyitaan. Permen 5 membagi dua macam data yang membutuhkan penetapan pengadilan negeri, dan yang tidak membutuhkan penetapan pengadilan negeri. Khusus untuk konten komunikasi, dibutuhkan penetapan pengadilan negeri. Sementara, KUHAP mengatur pengecualian atas

penetapan pengadilan bukan dari jenis barang yang disita, melainkan dari adanya unsur kebutuhan mendesak atau tidak. Ketentuan dalam KUHAP dipandang lebih sesuai dengan HAM apabila dibandingkan dengan Permen 5.

Akses terhadap sistem *vis-à-vis* penggeledahan. Akses terhadap sistem dapat dianalogikan suatu bentuk penggeledahan, dimana dalam hal ini APH masuk ke wilayah kerja/kediaman dari PSE. Wilayah kerja/kediaman yang dimaksud adalah sistem elektronik dari PSE yang bersangkutan. Dengan analogi ini, dapat dikaji pengaturan mengenai penyitaan dalam KUHAP, yaitu dalam Pasal 33 KUHAP, dimana dengan surat izin ketua pengadilan negeri setempat penyidik dalam melakukan penyidikan dapat mengadakan penggeledahan yang diperlukan. Selain itu, setiap kali memasuki rumah harus disaksikan oleh dua orang saksi dalam hal tersangka atau penghuni menyetujuinya dan juga harus disaksikan oleh kepala desa atau ketua lingkungan dengan dua orang saksi, dalam hal tersangka atau penghuni menolak atau tidak hadir. Jadi, prinsipnya penggeledahan itu dapat dilakukan dengan surat izin Ketua Pengadilan Negeri setempat. Tujuan keharusan adanya surat izin Ketua Pengadilan Negeri dalam tindakan penggeledahan rumah, dimaksudkan untuk menjamin hak asasi seseorang atas rumah kediamannya, juga agar penggeledahan tidak merupakan upaya yang dengan gampang dipergunakan penyidik tanpa pembatasan dan pengawasan.

Selanjutnya Pasal 34 KUHAP mengatur mengenai penggeledahan dalam keadaan mendesak, yaitu "*dalam keadaan yang sangat perlu dan mendesak bilamana penyidik harus segera bertindak dan tidak mungkin untuk mendapat surat izin terlebih dahulu, dengan tidak mengurangi ketentuan pasal 33 ayat (5) penyidik dapat melakukan penggeledahan untuk beberapa wilayah terbatas. Dan dalam hal inipun penyidik tidak diperkenankan memeriksa atau menyita surat, buku dan tulisan lain yang tidak merupakan benda yang berhubungan dengan tindak pidana yang bersangkutan atau yang diduga telah dipergunakan untuk melakukan tindak pidana tersebut dan untuk itu wajib segera melaporkan kepada ketua pengadilan negeri setempat guna memperoleh persetujuannya*."

Penjelasan Pasal 34 ayat (1) KUHAP menyatakan bahwa *keadaan yang sangat perlu* dan "*mendesak*" ialah bilamana di tempat yang akan digeledah diduga keras terdapat tersangka atau terdakwa yang patut dikhawatirkan segera melarikan diri atau mengulangi tindak pidana atau benda yang dapat disita dikhawatirkan segera dimusnahkan atau dipindahkan sedangkan surat izin dan ketua pengadilan negeri tidak mungkin diperoleh dengan cara yang layak dan dalam waktu yang singkat.

Dengan analogi ini, terlihat bahwa ada perbedaan antara akses terhadap sistem *vis-à-vis* penggeledahan. Akses terhadap sistem oleh kementerian/lembaga tidak membutuhkan penetapan dari pengadilan negeri. Ini berbeda dengan KUHAP yang mengharuskan adanya penetapan pengadilan guna menjamin HAM, kecuali untuk beberapa hal yang sifatnya mendesak.

Akses terhadap sistem. Berbagai literatur yang ada menunjukan bahwa terdapat pembahasan yang cukup banyak dari berbagai pakar terkait akses terhadap data elektronik. Namun, pembahasan terkait akses terhadap sistem elektronik sulit ditemukan baik dalam perdebatan teori maupun praktik di negara-negara. Akses terhadap sistem bukanlah praktik yang lazim karena memiliki risiko keamanan informasi yang cukup tinggi dan dapat menyebabkan gangguan kepada seluruh pengguna dari sistem, termasuk masyarakat (Rubinstein et al., 2014).

> Akses terhadap sistem bukanlah praktik yang lazim karena memiliki risiko keamanan informasi yang cukup tinggi dan dapat menyebabkan gangguan kepada seluruh pengguna dari sistem, termasuk masyarakat .

Permen 5 belum menjelaskan secara jelas tujuan dari akses terhadap sistem, dan dalam hal apa akses terhadap sistem elektronik dibutuhkan. Apabila tujuan akhirnya adalah untuk mendapatkan akses terhadap data, maka akses terhadap sistem elektronik hanya dilaksanakan sebagai upaya terakhir apabila pemerintah tidak mampu mendapatkan data yang sudah diakses.

Meskipun terlihat mirip, akses terhadap data dan akses terhadap sistem memiliki implikasi yang sangat berbeda. Akses terhadap sistem memiliki risiko keamanan informasi yang cukup tinggi, apalagi apabila tidak disertai dengan kontrol akses maupun langkah-langkah keamanan operasional yang diperlukan (OECD, 2019). Standar ISO/SNI 27001 tentang Sistem Manajemen Pengamanan Informasi (SMPI), sebagaimana sudah diadopsi oleh Badan Siber dan Sandi Negara, mengatur mengenai *access control* dan *operational security* untuk memastikan akses terhadap sistem elektronik dilaksanakan sesuai dengan prinsip-prinsip universal atas SMPI. Adapun berikut beberapa poin dalam SMPI yang relevan terkait dengan akses terhadap sistem:

Tabel 2.
Poin dalam Sistem Manajemen Pengamanan Informasi (SMPI) yang Berhubungan dengan Akses Terhadap Sistem

***Annex A9*: Access Control**	Pihak pengakses hanya dapat mengakses jaringan atau layanan jaringan apabila mendapatkan otorisasi yang spesifik. Akses harus dapat dikendalikan melalui prosedur login yang aman, dan terbatas sesuai dengan kebijakan access control.
Indikator	1. Adanya *multi factor authentication* 2. Adanya *unique credentials* 3. Adanya mekanisme verifikasi dan autentikasi 4. Larangan sharing login 5. Pengaturan akses jaringan berdasarkan job-role, dimana sistem admin dapat mengubah hak akses baik sementara atau permanen 6. Adanya pengakhiran sesi atau *log-off/log-out* secara otomatis setelah jangka waktu tertentu.

***Annex A12*: operations security**	Ketersediaan *event log* untuk mencatat aktivitas pihak pengguna, termasuk pengecualian, kesalahan, maupun insiden-insiden keamanan yang terjadi agar tercatat dan dikaji secara periodic.
Indikator	1. Atribusi durasi sesi dan tindakan dalam jaringan pada pengguna spesifik 2. Adanya pengawasan atas jaringan 3. Adanya pengawasan atas aktivitas dalam file atau folder, termasuk tindakan penyalinan, pemindahan, atau penghapusan 4. Adanya pelaporan dan audit keamanan berkala.

Sumber: Standar ISO/SNI 27001 tentang Sistem Manajemen Pengamanan Informasi (SMPI).

Dari standar-standar pada Annex A9 dan A12 SMPI ini, terlihat bahwa akses terhadap sistem memiliki risiko keamanan yang sangat tinggi. Ada kemungkinan pihak pengakses ternyata merupakan pihak yang tidak berwenang melakukan akses, baik karena terjadi peretasan, pemalsuan identitas, atau melakukan praktik *sharing login* misalnya di antara para petugas di kementerian atau lembaga (OECD, 2019). Apabila ini terjadi, risiko keamanan atas PSE meningkat pesat. Selain itu, dari sisi operasional juga dapat terjadi tindakan-tindakan yang membahayakan keamanan, seperti tindakan penyalinan atau penghapusan *file* atau *folder*, baik disengaja ataupun tidak disengaja.

Oleh karena itu, selain perlu tunduk pada prinsip-prinsip umum pemberian akses, khusus terkait hak akses terhadap sistem perlu juga dipastikan bahwa sistem PSE maupun petugas dari K/L yang melakukan akses terhadap sistem harus mematuhi prinsip-prinsip di bidang keamanan informasi, sekurang-kurangnya yang tercantum dalam ISO/SNI 27001. Dalam tataran praktis, perlu dikaji konsekuensi lebih lanjut hal ini, misalnya diperlukan audit terlebih dahulu atas APH atau K/L yang hendak melakukan akses terhadap sistem suatu PSE untuk memastikan bahwa sistem dan tindakan akses yang hendak mereka lakukan tidak bertentangan dengan praktik terbaik keamanan informasi.

“Oleh karena itu, selain perlu tunduk pada prinsip-prinsip umum pemberian akses, khusus terkait hak akses terhadap sistem perlu juga dipastikan bahwa sistem PSE maupun petugas dari K/L yang melakukan akses terhadap sistem harus mematuhi prinsip-prinsip di bidang keamanan informasi, sekurang-kurangnya yang tercantum dalam ISO/SNI 27001.”

Akses oleh APH vs. akses oleh kementerian atau lembaga. Apabila Ketentuan mengenai akses terhadap data/sistem dari APH memiliki perbandingan dari KUHAP, maka akses terhadap data/sistem dari kementerian atau lembaga tidak memiliki panduan yang seragam. Terlebih, dalam praktik terbaik internasional, kecuali untuk sektor keuangan, perpajakan, serta intelijen/keamanan negara, jarang ditemukan kewenangan bagi instansi pemerintah untuk melakukan akses data atau sistem (OECD, 2019). Ketentuan akses oleh kementerian atau lembaga dalam Permen 5 sebenarnya sudah bersumber dari Peraturan Pemerintah No 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Dalam Pasal 21 PP 71, disebutkan bahwa "Penyelenggara Sistem Elektronik Lingkup Privat wajib memberikan Akses terhadap Sistem Elektronik dan Data Elektronik dalam rangka **pengawasan** dan penegakan hukum sesuai dengan ketentuan peraturan perundang-undangan." Dalam hal ini berarti kebutuhan kementerian atau lembaga atas data atau sistem merupakan bagian dari pengawasan atas PSE yang bersangkutan. Namun demikian, Pasal 35 dari PP 71 menyatakan bahwa "ketentuan mengenai pengawasan atas Sistem Elektronik dalam sektor tertentu **wajib dibuat oleh Kementerian atau Lembaga** *terkait setelah berkoordinasi dengan Menteri*." Apabila ketentuan mengenai pengawasan dibuat oleh kementerian atau lembaga masing-masing, kehadiran pasal-pasal terkait akses terhadap data dan/atau sistem oleh kementerian atau lembaga dalam Permen 5 menjadi dapat diperdebatkan secara hukum. Mengingat hal ini, sebenarnya tidak ada delegasi kewenangan dari PP 71 kepada Kementerian Kominfo untuk mengatur lebih lanjut mengenai akses terhadap data atau sistem bagi kementerian atau lembaga.

Pendekatan dalam Pasal 35 dari PP 71 yang menyerahkan kepada kementerian atau lembaga masing-masing, dipandang lebih sesuai dengan praktik yang sudah ada di Indonesia maupun di luar negeri, dimana akses yang dilakukan oleh suatu kementerian atau lembaga umumnya dilandaskan pada suatu kewenangan yang melekat pada Undang-undang (yang pembuatannya sudah melalui proses politik melalui wakil rakyat di Dewan Perwakilan Rakyat), sehingga lebih mengakomodasi partisipasi publik. Dalam hal ini, sektor yang umumnya membutuhkan akses terhadap data adalah bidang perpajakan, jasa keuangan, dan keamanan negara atau intelijen. Di Indonesia, ketiga sektor ini juga sudah memiliki landasan hukum yang kuat setingkat UU yang menjadi dasar pengumpulan data untuk kepentingan-nya masing masing. Misalnya sebagai berikut:

- *Direktorat Jenderal Pajak*, untuk melakukan pemeriksaan perpajakan. Kewenangan ini sesuai dengan Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan sebagaimana telah beberapa kali diubah terakhir dengan UU tentang Cipta Kerja.
- *Otoritas Jasa Keuangan dan Bank Indonesia*, baik untuk kepentingan pengawasan/ pemeriksaan izin, maupun untuk pengawasan sistem keuangan dalam rangka melakukan penilaian terhadap risiko sistemik dan pemeriksaan untuk meyakini risiko sistemik. Kewenangan ini sesuai dengan UU tentang Bank Indonesia, UU tentang Otoritas Jasa Keuangan, berikut dengan PBI dan POJK terkait.
- *Badan Intelijen Negara*, untuk kegiatan yang mengancam kepentingan dan keamanan nasional meliputi ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan, dan sektor kehidupan masyarakat lainnya, termasuk pangan, energi, sumber daya alam, dan lingkungan hidup; dan/atau kegiatan terorisme, separatisme, spionase, dan sabotase yang mengancam keselamatan, keamanan, dan kedaulatan nasional, termasuk yang sedang menjalani proses hukum. UU No. 17 tahun 2011 tentang Intelijen Negara.

Di luar ketiga bidang ini, Indonesia memiliki preseden di bidang transportasi *online* untuk memberikan akses terhadap data kepada Pemerintah dalam bentuk *digital dashboard*. Dalam Peraturan Menteri Perhubungan No 11 2018 tahun Peraturan Menteri Perhubungan tentang Penyelenggaraan Angkutan Sewa Khusus, perusahaan aplikasi transportasi wajib membuat dan memberikan akses *digital dashboard* yang berisi data:

a. nama perusahaan, penanggungjawab, dan alamat Perusahaan Aplikasi;
b. data seluruh Perusahaan Angkutan Sewa Khusus yang bekerja sama;
c. data seluruh Kendaraan dan pengemudi;
d. akses monitoring operasional pelayanan berupa data transaksi pemesanan melalui aplikasi termasuk asal dan tujuan perjalanan dan tarif; dan,
e. layanan pengaduan konsumen berupa telepon dan surat elektronik Perusahaan Aplikasi.

Ketentuan akses data melalui *digital dashboard* dalam Peraturan Menteri Perhubungan 118 cukup detail dan setara dengan pemeriksaan pajak atau pemeriksaan dalam sektor keuangan. Apalagi data yang diminta menyangkut identitas pengemudi dan data transaksi pemesanan, yang menyentuh berbagai aspek perlindungan data pribadi, maupun data yang tergolong sebagai rahasia dagang perusahaan. Apabila tidak dikelola dengan baik, ada potensi data ini disalahgunakan untuk persaingan usaha yang tidak sehat, misalnya untuk melihat penetrasi pesaing di berbagai wilayah di Indonesia. Permasalahannya, ketentuan mengenai *digital dashboard* tidak dilandasi dengan dasar hukum yang eksplisit dalam UU tentang Lalu Lintas dan Angkutan Jalan No. 22 tahun 2009. Peraturan Menteri Perhubungan 118 bahkan tidak merujuk sama sekali UU ini.

Di luar dari ketiga bidang umum dan satu bidang khusus aplikasi transportasi di Indonesia, akses terhadap permintaan data dari kementerian lembaga umumnya berkait dengan pengawasan atas izin. Kementerian atau lembaga dapat meminta dokumen pendukung, atau juga melakukan pemeriksaan lapangan, dalam memastikan kepatuhan terhadap suatu izin usaha.

Dengan beragamnya tipologi akses oleh K/L untuk kepentingan pengawasan, demi memastikan praktik yang sudah berjalan selama ini lancar dan mencegah multi-tafsir atas kewenangan, serta juga untuk mematuhi semangat Pasal 35 dari PP 71, Kementerian Kominfo secara umum dan Permen 5 secara khusus perlu ditempatkan sebagai instrumen yang membina dan memastikan setiap permintaan akses data dari K/L harus menghormati prinsip perlindungan terhadap data pribadi, selain ketentuan spesifik di sektornya masing-masing.

“Dengan beragamnya tipologi akses oleh K/L untuk kepentingan pengawasan, demi memastikan praktik yang sudah berjalan selama ini lancar dan mencegah multi-tafsir atas kewenangan, serta juga untuk mematuhi semangat Pasal 35 dari PP 71, Kementerian Kominfo secara umum dan Permen 5 secara khusus perlu ditempatkan sebagai instrumen yang membina dan memastikan setiap permintaan akses data dari K/L harus menghormati prinsip perlindungan terhadap data pribadi, selain ketentuan spesifik di sektornya masing-masing.”

Ketika Kominfo dan Permen 5 ditempatkan sebagai instrumen Pembina dan harmonisasi, maka Permen 5 seharusnya tidak menciptakan norma hukum baru. Namun, Permen 5 lebih diarahkan sebagai petunjuk teknis untuk mengatur hubungan dan koordinasi antara Lembaga, misalnya, *pertama*, hubungan antara Kominfo dan APH. Dalam hal ini, Kominfo dapat berperan sebagai *privacy safeguard* untuk memastikan akses yang aman dari APH. *Kedua*, hubungan antara Kominfo dengan K/L pengawas. Dalam hal ini, Kominfo juga dapat berperan sebagai *privacy safeguard* dan sewajarnya dapat menyeragamkan prosedur hak akses dari instansi-instansi yang diberikan kewenangan untuk itu sesuai UU sektoral-nya. *Ketiga*, hubungan antara Kominfo dengan penyidik pegawai negeri sipil, atau PPNS. PPNS memiliki posisi yang unik karena bekerja berdasarkan UU sektoral, namun tetap berkoordinasi dengan kepolisian. Dengan struktur yang serupa, Kominfo dapat menjadi poros koordinasi bagi PPNS untuk melakukan akses terhadap data dan sistem elektronik.

Pengujian atas substansi dan formalitas permohonan akses. Seandainya pun sudah disusun pengaturan yang lengkap mengenai hak akses atas data atau sistem, dalam praktik akan banyak terdapat perdebatan atau penafsiran mengenai kewenangan dari suatu kementerian, lembaga, atau APH. Hal ini wajar mengingat data atau sistem elektronik merupakan aset terbesar dari PSE yang memiliki dimensi kerahasiaan dan kekayaan intelektual yang kompleks (Accenture, 2016). Apabila kita menganalogikan akses atas data dan sistem dengan penyitaan dan penggeledahan, maka untuk mendukung adanya *due process* serta *checks and balances*, setiap hak atas akses perlu juga dilengkapi dengan sarana mengajukan keberatan atau pengaduan layaknya praperadilan dalam KUHAP. Berdasar pasal 77 huruf a KUHAP, praperadilan adalah wewenang pengadilan negeri untuk memeriksa dan memutus sah atau tidaknya penangkapan, penahanan, penghentian penyidikan atau penghentian penuntutan. Mahkamah Konstitusi telah memberikan tambahan wewenang terhadap praperadilan dalam putusannya No. 21/PUU-XII/2014 sehingga praperadilan juga berwenang untuk memeriksa dan memutus sah atau tidaknya penetapan tersangka, penggeledahan atau penyitaan.

Permen 5, dalam hal ini, belum mengatur mengenai mekanisme untuk mengajukan keberatan dan menguji apakah:

a. Dasar kewenangan dari kementerian atau lembaga atau APH sudah tepat?
b. Maksud, tujuan, dan kepentingan dari kementerian atau lembaga atau APH sudah tepat?
c. Jenis akses yang diminta sudah relevan dengan dasar kewenangan maupun maksud dan tujuan?

BEBERAPA CONTOH PERBANDINGAN DI NEGARA LAIN DAN PERAN PELAKU USAHA

Storage Communication Act (SCA), Perlindungan Data Pribadi, dan Kasus Microsoft

Di Amerika Serikat, perlindungan terhadap hak atas privasi diatur dalam Amandemen keempat Konstitusi AS, dan diatur lebih lanjut dalam the *Electronic Communications Privacy Act* (ECPA) (Department of Justice, n.d.). Perubahan ECPA di tahun 1986 memperkenalkan aturan khusus mengenai *Stored Communication Act* (SCA) yang berfungsi sebagai *lex specialis*. SCA membatasi tindakan pemerintah untuk mengakses data terkait informasi pengguna. Dalam hal ini, untuk semua kasus pemeriksaan, termasuk gugatan perdata atau gugatan administrasi negara, maka lembaga negara membutuhkan *subpoena* dari pengadilan untuk mendapatkan informasi pendaftaran pengguna dan juga untuk mendapatkan data IP address (Schwartz Hannum PC, 2015). *Subpoena* adalah permohonan yang dapat diajukan oleh siapapun (baik individu, swasta, ataupun lembaga negara) untuk mendapatkan akses informasi terhadap pihak lawan sengketanya.

Sementara itu, khusus untuk perkara pidana, dibutuhkan dokumen pengadilan yang lebih kuat dari *subpoena* (Turner, 2016). SCA mengatur bahwa untuk mendapatkan data non-konten, dibutuhkan perintah dari pengadilan. Informasi non-konten termasuk alamat tujuan, pengirim, CC/BCC, atau *times-stamp* dari suatu surat elektronik. Sedangkan untuk informasi konten dari suatu surat elektronik, maka dibutuhkan *search warrant*, yang membutuhkan beban pembuktian lebih besar dari penyidik atau penuntut berupa adanya "*probable cause*", untuk membuktikan justifikasi atas konten yang diminta.

Sebagai contoh, Google secara eksplisit menyatakan kepatuhannya terhadap ECPA dan SCA dalam laman *information request* (Google, n.d.). Facebook juga dalam laman yang serupa menyatakan sebagai berikut (Facebook, n.d.):

> *"We disclose account records solely in accordance with our terms of service and applicable law, including the United States Federal Stored Communications Act ("SCA"), 18 USC sections 2701-2712. Under US law:*
>
> - *A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 USC section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es) and a recent login/logout IP address(es), if available.*
> - *A court order issued under 18 USC section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.*
> - *A search warrant issued under the procedures described in the United States Federal Rules of Criminal Procedure or equivalent local warrant procedures upon presentation of a probable cause is required to compel the disclosure of the stored contents of any*

account, which may include messages, photos, videos, Timeline posts and location information."

Dari praktik di AS, dapat diketahui bahwa setiap permohonan akses membutuhkan persetujuan/penetapan dari pengadilan. Hanya saja beban pembuktian untuk informasi tertentu dianggap lebih ringan sehingga ada yang membutuhkan dokumen *subpoena*, dan ada yang membutuhkan dokumen *search warrant* yang perlu menguji adanya *probable cause*.

Satu hal yang perlu pula dipahami adalah SCA tidak membeda-bedakan antara akses oleh APH dan akses oleh kementerian atau lembaga. Hal ini karena setiap kepentingan pemeriksaan atau pengawasan dari kementerian atau lembaga tetap diselenggarakan dengan menempuh jalur hukum, baik dalam konteks pengadilan perdata, administrasi/tata usaha negara, ataupun pidana. Ini berbeda dengan sistem hukum di Indonesia yang memungkinkan adanya proses pemeriksaan hukum tanpa pengadilan, meskipun dimungkinkan pihak yang berkeberatan mengajukan gugatan perdata atau tata usaha negara dalam hal berkeberatan atas proses pemeriksaan.

Meskipun sudah mengatur cukup rinci mengenai akses terhadap data, SCA masih dianggap belum sempurna terutama dalam perspektif perlindungan data pribadi. Satu hal yang belum diatur adalah kewajiban untuk memberitahu pengguna dalam hal suatu perusahaan teknologi menerima permohonan akses dari APH.

Satu kasus yang cukup menarik perhatian adalah kasus Microsoft Corporation v. US (2016), dimana Microsoft memohon penetapan pengadilan yang diajukan di Pengadilan Distrik AS di Seattle, Washington (Columbia University Global Freedom of Expression, 2016). Permasalahan yang menjadi obyek sengketa adalah SCA tahun 1986 dengan Microsoft yang menyatakan bahwa perintah kerahasiaan atau *secrecy order* dari *Department of Justice* (Kementerian Hukum - DoJ) mencegah mereka mengungkapkan *search warrant* yang mereka terima dari penuntut umum DoJ kepada pelanggan mereka. Menurut Microsoft, *secrecy order* bertentangan dengan kewajiban mereka untuk menjaga privasi pelanggannya. Kasus ini dimulai pada April 2016, dan Microsoft dalam gugatannya didukung oleh perusahaan seperti Amazon, Apple, Google, Dropbox dan Salesforce. Pada bulan Oktober 2017, Microsoft menarik kembali gugatan ini setelah DoJ memutuskan untuk mengubah kebijakan mereka terkait notifikasi kepada pengguna atau subjek data pribadi. Meskipun tidak ada undang-undang yang diubah, kebijakan *Department of Justice* yang baru "mengubah aturan permintaan data terkait notifikasi kepada pengguna Internet tentang lembaga pemerintah yang mengakses informasi mereka," serta mengamanatkan pembatasan periode waktu seandainya diperlukan penerbitan *secrecy order*.

Dalam upaya untuk mengajukan keberatan atas pengaturan-pengaturan di dalam SCA, Microsoft berpandangan bahwa ketentuan yang ada dalam SCA belum cukup mengakomodasi kebutuhan dunia usaha. Untuk memastikan *trust* tetap terjaga antara perusahaan teknologi dengan penggunanya, Microsoft mengusulkan agar ada tiga prinsip tambahan yang dapat dijadikan acuan.

Pertama, transparansi, dimana pengguna berhak untuk mengetahui ketika pemerintah meminta hak akses atas catatan atau konten komunikasi emailnya. *Kedua*, netralitas digital. Artinya, hanya karena suatu data terdapat secara elektronik atau disimpan di penyimpanan awan (*cloud*), bukan berarti perlindungannya menjadi lebih lemah. Seyogyanya prinsip perlindungan hukum

tetap berlaku setara terlepas teknologi yang digunakan. *Ketiga*, justifikasi. seandainya pun ada justifikasi untuk merahasiakan akses kepada pengguna, maka hal ini harus disesuaikan dengan kebutuhan atau kepentingan dari kasus penyidikan yang sedang dijalankan. Apabila pemerintah tidak dapat memberikan justifikasi yang tepat, perusahaan seperti Microsoft wajib memberitahukan akses kepada penggunanya (Smith, 2016).

Sejak adanya gugatan dari Microsoft, penuntut umum dari DoJ mengubah praktik mereka untuk tunduk terhadap prinsip-prinsip umum perlindungan data pribadi.

Contoh dari Beberapa Praktik di Negara Lain

Pengalaman dari beberapa negara lain di dunia menunjukan bahwa akses Pemerintah terhadap data elektronik cukup banyak ditemukan. Namun, dari semua contoh-contoh ini, terdapat kesamaan pendekatan, yaitu akses terhadap data selalu dilandasi pada legislasi setingkat Undang-undang.

Di Korea Selatan, misalnya, akses Pemerintah terhadap data dapat ditemukan di berbagai peraturan perundang-undangan, khususnya *Act on Personal Information Protection of Public Agencies* (APIPPA) yang pada tahun 2011 diganti dan digabung dengan *Personal Information Protection Act* (PIPA) dan *Telecommunications Business Act* (TBA). Selain PIPA dan TBA, sejumlah undang-undang lainnya, termasuk *Credit Information Act*, *Communication Privacy Act*, *the Real Name Finance Act*, dan *Act on Use and Protection of DNA Identification Information* (*DNA Identification Act*), mengatur penyitaan data dengan surat perintah atau cara lain.Terkait data transaksional, *Communication Privacy Act* mewajibkan otoritas penegak hukum untuk memberi tahu subjek data secara tertulis dalam waktu 30 hari setelah mendapatkan catatan untuk tujuan penyelidikan (Jong, 2017).

Dalam TBA terdapat rincian data yang disediakan oleh operator telekomunikasi untuk memenuhi permintaan penyediaan data komunikasi dari pengadilan, jaksa, atau kepala badan intelijen, jika diperlukan untuk persidangan, investigasi kejahatan, atau keamanan nasional. Data tersebut mencakup nama pengguna, nomor registrasi penduduk pengguna, alamat pengguna, nomor telepon pengguna, kode identifikasi yang digunakan untuk mengidentifikasi pengguna jaringan komunikasi yang sah, dan tanggal pengguna memulai atau menghentikan langganan mereka. Sehubungan dengan anti-terorisme, untuk memiliki akses ke konten komunikasi, informasi perjalanan, dan informasi keuangan, Badan Intelijen Nasional (NIA) Korea dapat tanpa surat perintah pengadilan untuk meminta ISP untuk memberikan informasi kontak, informasi lokasi, dan informasi pribadi lain yang relevan mengenai tersangka teroris.

Untuk akses data untuk kepentingan pengawasan regulator, salah satu contohnya adalah informasi pribadi mengenai pelanggar hak cipta yang diserahkan kepada Menteri Kebudayaan, Olahraga dan Pariwisata. Untuk melindungi hak cipta, Undang-Undang Hak Cipta Korea memberikan otoritas kepada menteri untuk menuntut Penyedia Layanan Internet (ISP) menghapus atau menghentikan transmisi reproduksi ilegal atau untuk menangguhkan akun pelanggar untuk layanan online selama jangka waktu terbatas. Selanjutnya, atas permintaan pemegang hak cipta yang mencari data untuk tuntutan hukum, menteri dapat memerintahkan ISP untuk memberikan daftar orang-orang yang dicurigai memiliki salinan atau mengirimkan reproduksi ilegal.

Di India, ditemukan ketentuan akses data untuk penegakan hukum dalam Bab 91 dari *Code of Criminal Procedure*, 1973 (CrPc) (Abraham, 2017). Kemudian, menurut bawah *Reserve Bank Act*, agar pemerintah dapat mengakses dokumen keuangan, pemerintah harus meminta akses dari Bank Sentral India, atau mendapatkan perintah pengadilan dan meminta informasi dari cabang bank itu sendiri. Sebagai pengamanan untuk mengakses, ketentuan dari *Bankers Book Evidence Act* berlaku untuk semua informasi atau dokumen yang disimpan oleh penyedia sistem. *Securities and Exchange Board of India* atau SEBI juga memiliki akses luas ke data sektor swasta diberi wewenang yang sama seperti pengadilan, termasuk mewajibkan pembukaan buku rekening dan dokumen lainnya.

Information Technology Act (ITA) 2008 memberikan kewenangan bagi badan keamanan pemerintah akses ke informasi pengguna yang dipegang oleh sektor swasta untuk kepentingan penyidikan (Abraham, 2017). Dalam bab "Perlindungan Data" dan aturan "Praktik dan Prosedur Keamanan yang Wajar dan Informasi Pribadi yang Sensitif", akses oleh pemerintah diizinkan secara luas, yakni (a) tidak mewajibkan badan keamanan untuk mendapatkan otorisasi sebelum mengakses informasi; (b) mengizinkan akses ke badan pemerintah mana pun; (c) mengizinkan akses ke semua jenis "data atau informasi pribadi sensitif"; dan (d) mengizinkan data yang diakses digunakan untuk tujuan yang luas dan umum.

Di Brazil pada tahun 2014, dikeluarkan undang-undang untuk mengatur penggunaan Internet, *Marco Civil da Internet* (Magrani, 2017). Undang-undang ini memberikan aturan yang menangani akses oleh penegak hukum ke data pribadi, konten komunikasi, informasi identitas pelanggan (alamat IP), dan data pendaftaran dari telekomunikasi dan penyedia *online*. Terkait kerahasiaan data keuangan, data keuangan hanya dapat diperoleh dengan surat perintah pengadilan, jika diperlukan untuk investigasi tindak pidana. Undang-undang tersebut memungkinkan *Brazil Revenue Service* (BRS) untuk meminta dan memperoleh informasi keuangan langsung dari lembaga keuangan terlepas dari otorisasi yudisial.

Dalam karya ilmiahnya, Magrani (2017) memberikan tipologi otorisasi yang diperlukan untuk mendapatkan akses terhadap data sebagai berikut:

Tabel 3.
Tipologi Otorisasi yang Diperlukan untuk Mendapatkan Akses Terhadap Data

Tipe Data/Tipe Kewenangan yang Dibutuhkan untuk Mengakses Data Tersebut	Apakah Akses Membutuhkan Izin dari Pengadilan?	Apakah Permintaan Akses Data dari Polisi dan Kejaksaan Sudah Cukup?	Badan Regulator Dapat Mengakses Data dengan Tujuan hanya untuk Mengawasi Aktivitas yang Diatur Badan Tersebut
Konten Komunikasi	Ya	Tidak	Tidak
Metadata Komunikasi	Ya	Tidak	Tidak
Data Pendaftaran	Tidak	Ya	Ya
Non-komunikasi; Transaksi atau pencatatan bisnis	Ya	Kurang Jelas	Ya

Sumber: Magrani (2017).

Di Tiongkok, *State Security Law* 1993 memberikan kewenangan organisasi keamanan negara untuk mengakses informasi atau data apa pun yang dipegang oleh siapa pun di Tiongkok (Wang, 2017). Pasal 28 *Law on Guarding State Secrets* (Revisi 2010) juga menetapkan bahwa "Operator dan penyedia layanan Internet atau jaringan informasi publik lainnya harus bekerja sama dengan organisasi keamanan publik, organisasi keamanan nasional, dan organisasi kejaksaan dalam penyelidikan kasus kebocoran rahasia (Wang, 2017)".

Salah satu proyek besar di Tiongkok adalah proyek *Golden Shield* yang dimotori oleh Kementerian Keamanan Publik (MPS) ditambah 11 lembaga lainnya seperti Administrasi Perpajakan Negara, Bea Cukai, dan Bank Sentral (PBOC), Kementerian Perindustrian dan Teknologi Informasi. (MIIT), dan lembaga lainnya. Ke-12 lembaga ini menjadi bagian dari inisiatif untuk membangun sistem *e-government*. Proyek dan database ini mengacu pada kerangka kerja yang ditetapkan oleh *Guiding Opinion on Construction of E-Government in our Country* yang dikeluarkan *State Informatisation Leading Group*. Salah satu basis data Proyek *Golden Shield* adalah Basis Data Internet Dasar yang tersusun dari data yang dikumpulkan setiap bulan sejak 2006 dari ISP (Penyedia Layanan Internet), ICP (Penyedia Konten Internet), IDC (Pusat Data Internet), dan layanan email. Tidak ada kewenangan eksplisit untuk membangun database ini yang dapat ditemukan di undang-undang mana pun, dan hanya ada surat perintah dari polisi setempat yang meminta bisnis untuk menyerahkan laporan bulanan dengan templat pengumpulan data yang dirancang oleh MPS. Data yang dikumpulkan mencakup semua akun pengguna dan informasi pendaftaran, baik individu maupun perusahaan, dan data lain yang diminati pemerintah.

REKOMENDASI KEBIJAKAN

Dari pembahasan aspek legal dan kebijakan publik dalam kajian ini, disimpulkan bahwa ketentuan mengenai akses data/sistem sebagaimana diatur dalam Peraturan Menteri Komunikasi dan Informatika No. 5 tahun 2020 tentang Penyelenggara Sistem Elektronik (PSE) Lingkup Privat merupakan bidang perdebatan yang cukup dinamis tidak hanya di Indonesia maupun di seluruh dunia. Di satu sisi, terdapat kebutuhan yang sah dari lembaga negara untuk mengakses data dari PSE atau *platform* digital. Di sisi lain, dibutuhkan prinsip-prinsip dasar yang melandasi akses ini agar kepentingan HAM dan perlindungan data pribadi tetap terjaga dengan baik.

Permen 5 sebenarnya sudah membahas beberapa prinsip ini. Misalnya, sudah disebutkan ke butuhan penilaian (*assessment*) atas kepentingan pengawasan dan proporsionalitas serta legalitas, dan juga perlu disebutkan secara eksplisit ruang lingkup atau jenis sistem atau data elektronik yang hendak diakses. Akses juga hanya dapat digunakan untuk kepentingan yang disebutkan dalam permintaan. Prinsip perlindungan data pribadi dan keamanan informasi memang sudah disebutkan secara eksplisit.

Namun demikian, masih dibutuhkan ketentuan-ketentuan prinsipil dan operasional yang lebih detail untuk memastikan terlindunginya HAM dan data pribadi dari pengguna. Atas dasar ini, kajian ini memberikan beberapa rekomendasi sebagai berikut.

Perlunya penyempurnaan untuk memastikan *Due process of law*, khususnya untuk aspek:

a. Legalitas: akses terhadap data dan sistem elektronik berkaitan dengan prinsip dasar HAM, perlindungan data pribadi, dan juga perlindungan rahasia dagang milik PSE. Oleh karena itu, pengaturan mengenai hal ini seyogyanya diatur di tingkat Undang-undang. Pengaturan dalam tingkat UU memungkinkan ruang diskusi dengan melibatkan wakil rakyat di parlemen. Berkaca dari pengalaman dari Korea Selatan, India, dan Brazil. Meskipun memiliki pendekatan yang berbeda, di negara-negara ini terdapat kesamaan yaitu adanya landasan hukum di tingkat Undang-undang. Satu program yang tidak memiliki landasan legalitas yang jelas adalah proyek *Golden Shield* di Tiongkok, yang mana banyak mendapat berbagai pertentangan dari pemangku kepentingan.

b. Otorisasi atau penetapan dari badan peradilan/badan independen: Permen 5 membedakan data yang membutuhkan penetapan pengadilan dan yang tidak membutuhkan. Hal ini berbeda dengan semangat KUHAP yang mensyaratkan penetapan pengadilan untuk penyitaan dan penggeledahan, kecuali untuk hal-hal yang mendesak. Permen 5 seyogyanya mengadopsi semangat ini, dimana semua akses membutuhkan penetapan pengadilan atau badan independen lainnya, kecuali untuk urusan-urusan tertentu yang disebutkan secara spesifik dalam Undang-undang.

c. Pengujian dan keberatan: dalam perkembangannya sangat dimungkinkan terjadi perdebatan atau keberatan dari PSE atas suatu permohonan akses. Untuk memastikan dilindunginya hak-hak asasi dari pengguna maupun hak dasar dari PSE, perlu disediakan

sarana untuk menguji atau mengajukan keberatan melalui suatu badan atau forum yang netral, seperti pengadilan. Ini serupa dengan proses pra-peradilan dalam KUHAP, atau adanya suatu forum pengujian atas keputusan hak akses melalui peradilan tata usaha negara.

Kementerian Kominfo perlu berperan sebagai Pembina dan pelindung untuk memastikan akses oleh K/L sesuai dengan prinsip perlindungan data pribadi.

Mengingat beragamnya ketentuan dalam UU sektoral, akses oleh kementerian atau lembaga dapat membuka multi penafsiran atas lembaga-lembaga pemerintah yang berwenang melakukan akses. Idealnya, seyogyanya UU Perlindungan Data Pribadi sah dan berlaku terlebih dahulu sebelum kewenangan hak akses oleh pemerintah dapat berjalan dengan baik. Dalam situasi saat ini, Kementerian Kominfo perlu menempatkan Permen 5 sebagai instrumen kebijakan yang memastikan setiap permintaan akses dari K/L sesuai dengan prinsip perlindungan data pribadi dan keamanan informasi. Kominfo juga dapat menempatkan Permen 5 bukan sebagai pencipta norma baru melainkan sebagai aturan teknis yang mengatur operasional hubungan antara Kominfo dengan aparat penegak hukum dan K/L lain (termasuk dengan PPNS dan BSSN), yang selama ini masih memiliki praktik beragam di lapangan.

Akses terhadap sistem PSE sebaiknya dijadikan alternatif terakhir dan semua langkah mitigasi risiko sudah dijalankan.

Permen 5 belum menjabarkan tujuan dari akses terhadap sistem, dan bilamana akses terhadap sistem diperlukan. Akses terhadap sistem elektronik bukanlah merupakan *best practice* di bidang keamanan informasi karena membuka celah baru yang berisiko bagi sistem PSE. Akses terhadap sistem wajib tunduk terhadap aturan internasional seperti ISO/SNI SMPI, khususnya mengenai *access control* dan *security operations*. Dalam hal ini, lembaga negara yang hendak mengakses sistem juga perlu tunduk dan di-audit SMPI sebelum melakukan akses terhadap sistem PSE.

REFERENSI

Abraham, S. (2017). Systematic Government Access to Private- Sector Data in India. In F. H. Cate & J. X. Dempsey (Eds.), Bulk Collection: Systematic Government Access to Private-Sector Data (pp. 259–274). Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-12

Accenture. (2016). *The Ethics of Data Sharing: A guide to best practices and governance*.

Ackerman, S. (2014, January 27). *Tech giants reach White House deal on NSA surveillance of customer data*. https://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data

Columbia University Global Freedom of Expression. (2016, July 14). *Microsoft v. United States*. Case Law. https://globalfreedomofexpression.columbia.edu/cases/microsoft-v-united-states/

Cornell Law School. (n.d.). *National Security Letter*. Retrieved April 30, 2021, from https://www.law.cornell.edu/wex/national_security_letter

Daskal, J., & Woods, A. K. (2015, November 24). *Cross-Border Data Requests: A Proposed Framework - Just Security.* https://www.justsecurity.org/27857/cross-border-data-requests-proposed- framework/

Department of Justice. (n.d.). *Electronic Communications Privacy Act of 1986 (ECPA)*. Retrieved April 30, 2021, from https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Facebook. (n.d.). *Information for Law Enforcement Authorities*. Retrieved April 30, 2021, from https://www.facebook.com/safety/groups/law/guidelines/?_rdr

Global Network Initiative. (2018). *Implementation Guidelines for the Principles on Freedom of Expression and Privacy*. https://globalnetworkinitiative.org/wp-content/uploads/2018/08/Implementation-Guidelines-for-the-GNI-Principles.pdf

Google. (n.d.). *How Google handles government requests for user information*. Retrieved April 30, 2021, from https://policies.google.com/terms/information-requests

Jong, S. J. (2017). Systematic government access to private-sector data in the Republic of Korea. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 287–303). Oxford University Press. https://doi.org/10.1093/idpl/ipt030

Magrani, B. (2017). Systematic Government access to private-sector data in Brazil. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 129–146). Oxford University Press. https://doi.org/10.1093/idpl/ipt033

Nissenbaum, H., Strandburg, K., & Brennan-Marquez, K. (n.d.). *Metadata Project*. Retrieved April 30, 2021, from https://www.law.nyu.edu/centers/ili/metadataproject

OECD. (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: a comparative analysis †. *International Data Privacy Law*, *4*(2). https://academic.oup.com/idpl/article/2/4/195/676962

Schwartz Hannum PC. (2015). *Stored Communications Act Does Not Permit Service Providers to Disregard Subpoenas for E-Mails | Schwartz Hannum PC*. http://www.shpclaw.com/Schwartz-Resources/stored-communications-act-does-not-permit-service-providers-to-disregard-subpoenas-for-e-mails?p=11399

Smith, B. (2016, April 14). *Keeping secrecy the exception, not the rule: An issue for both consumers and* businesses.

https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/#sm.00001qg545hu8ldwmw7h8092g7f67

Turner, S. A. (2016). *Are Changes in Store for the Stored Communications Act?* http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf.

van Eijk, N. (2017). Standards for Independent Oversight. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-sector Data* (pp. 381–393). Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-20

Wang, Z. (2017). Systematic government access to private-sector data in China. In F. H. Cate & J. X. Dempsey (Eds.), *Bulk Collection: Systematic Government Access to Private-Sector Data* (pp. 241–258). Oxford University Press. https://doi.org/10.1093/idpl/ips017

Yeh, B. T., & Doyle, C. (2006). *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*.

TENTANG PENULIS

Ajisatria Suleiman merupakan praktisi bidang regulasi kebijakan publik dengan spesialisasi Ekonomi Digital dan Keuangan Digital. Dalam kariernya, Ia telah membantu mengembangkan internet secara regional dan nasional, serta bekerja sama dengan asosiasi industri keuangan digital, badan pengembangan internasional, perusahaan teknologi berbasis global, dan perusahaan rintisan lokal.

Fokus penelitiannya adalah perlindungan data pribadi, kedaulatan digital, dan keuangan digital.

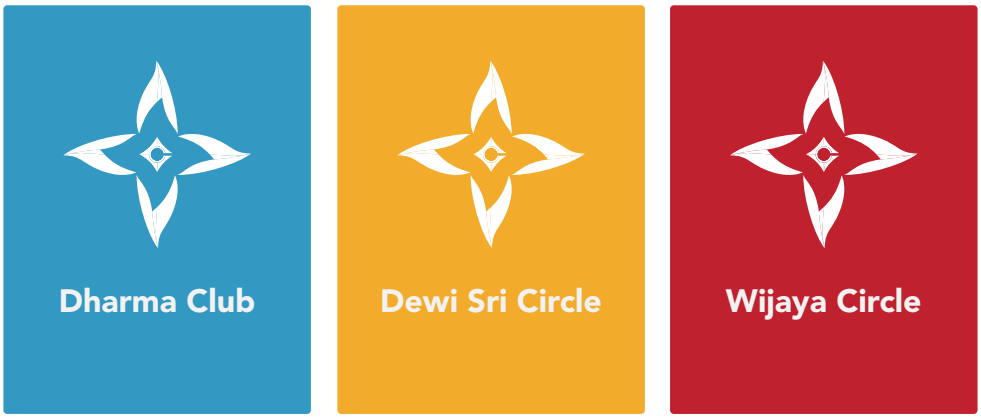
Ia mendapatkan gelar Sarjana Hukum dari Universitas Indonesia, dan gelar Master dari Erasmus University of Rotterdam dan University of Hamburg.

AYO BERGABUNG DALAM PROGRAM "*SUPPORTERS CIRCLES*" KAMI

Melalui *Supporters Circles*, kamu, bersama dengan ratusan lainnya, membantu kami untuk melakukan penelitian kebijakan serta advokasi untuk kemakmuran jutaan orang di Indonesia yang lebih baik.

Dengan bergabung dalam *Supporters Circles*, *supporters* akan mendapatkan keuntungan dengan terlibat lebih dalam di beberapa karya CIPS. *Supporters* bisa mendapatkan:

- Undangan Tahunan *Gala Dinner* CIPS
- Pertemuan eksklusif dengan pimpinan CIPS
- Mendapatkan prioritas pada acara-acara yang diadakan oleh CIPS
- Mendapatkan informasi terbaru secara personal, setiap satu bulan atau empat bulan, lewat email dan video mengenai CIPS
- Mendapatkan *hard-copy* materi publikasi CIPS (lewat permintaan)



Untuk informasi lebih lanjut, silahkan hubungi anthea.haryoko@cips-indonesia.org.

Pindai untuk bergabung

TENTANG 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. Kami didukung secara finansial oleh para donatur dan filantropis yang menghargai independensi analisi kami.

FOKUS AREA CIPS:

Ketahanan Pangan dan Agrikultur: Memberikan akses terhadap konsumen di Indonesia yang berpenghasilan rendah terhadap bahan makanan pokok dengan harga yang lebih terjangkau dan berkualitas. CIPS mengadvokasi kebijakan yang menghapuskan hambatan bagi sektor swasta untuk beroperasi secara terbuka di sektor pangan dan pertanian.

Kebijakan Pendidikan: Masa depan SDM Indonesia perlu dipersiapkan dengan keterampilan dan pengetahuan yang relevan terhadap perkembangan abad ke-21. CIPS mengadvokasi kebijakan yang mendorong sifat kompetitif yang sehat di antara penyedia sarana pendidikan. Kompetisi akan mendorong penyedia sarana untuk terus berupaya berinovasi dan meningkatkan kualitas pendidikan terhadap anak-anak dan orang tua yang mereka layani. Secara khusus, CIPS berfokus pada peningkatan keberlanjutan operasional dan keuangan sekolah swasta berbiaya rendah yang secara langsung melayani kalangan berpenghasilan rendah.

Kesejahateraan Masyarakat: CIPS mempercayai bahwa komunitas yang solid akan menyediakan lingkungan yang baik serta mendidik bagi individu dan keluarga mereka sendiri. Kemudian, mereka juga harus memiliki kapasitas untuk memiliki dan mengelola sumber daya lokal dengan baik, berikut dengan pengetahuan mengenai kondisi kehidupan yang sehat, agar mereka bisa mengelola pembangunan dan kesejahteraan komunitas dengan baik.

www.cips-indonesia.org

facebook.com/cips.indonesia

@cips_id

@cips_id

Center for Indonesian Policy Studies

Center for Indonesian Policy Studies

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