6 Januari 2021

Yth.

Bpk. Johny G. Plate
Menteri Komunikasi dan Informatika
Kementerian Komunikasi dan Informatika (KOMINFO)
Jl. Medan Merdeka Barat no. 9, Jakarta 10110 Indonesia

Bpk. Semuel A. Pangerapan
Direktur Jenderal Penerapan Informatika
Kementerian Komunikasi dan Informatika

Perihal: Masukan Industri terkait Peraturan Menteri Kominfo No. 5/2020 ("PM 5")

Kepada Bapak Menteri yang terhormat,

The Asia Internet Coalition (AIC) dan para anggotanya ingin menyampaikan rekomendasi kami dan meminta klarifikasi atas diterbitkan baru-baru ini **Peraturan Menteri No. 5/2020 yang("PM 5")** pada tanggal 2 Desember 2020, tentang Penyelenggara Sistem Elektronik Lingkup Privat oleh Kementerian Komunikasi dan Informatika (Kominfo). Kami memahami bahwa PM 5 merupakan salah satu peraturan pelaksana berdasarkan Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71).

AIC adalah asosiasi industri yang terdiri dari perusahaan Internet dan teknologi terkemuka. Sebagai mitra terpercaya untuk Kominfo dan Pemerintah Indonesia, AIC berupaya untuk mendorong pemahaman dan penyelesaian masalah kebijakan Internet dan TIK di kawasan Asia Pasifik. Perusahaan anggota kami ingin meyakinkan Pemerintah bahwa kami akan terus berkontribusi aktif dalam keamanan platform digital, produk, dan layanan dalam mendukung tujuan ekonomi digital Indonesia. Banyak dari perusahaan anggota kami merupakan kontributor substansial bagi sektor teknologi informasi dan komunikasi (TIK) Indonesia yang dinamis. Bagi kita semua, Indonesia adalah pasar yang penting.

Meskipun kami mengapresiasi upaya Pemerintah Indonesia dan KOMINFO dalam menyusun Peraturan Menteri No. 5/2020, kami sangat yakin bahwa ada kekhawatiran dan klarifikasi yang diperlukan terkait ketentuannya, dan menyarankan agar mereka selaras dengan praktik terbaik industri untuk mendorong berkembangnya ekonomi digital. di Indonesia. Pertama, Kami prihatin dengan luasnya cakupan definisi Penyelenggara Sistem Elektronik (PSE), yang pada dasarnya mencakup sebagian besar, jika tidak semua, jenis PSE di Indonesia yang mungkin tidak menimbulkan risiko bagi keamanan nasional Indonesia, menyebabkan keresahan sosial dan

politik, atau pelanggaran data pribadi. Potensi penyertaan entitas luar negeri juga menjadi perhatian, bersama dengan proses pendaftaran yang detailnya belum tidak jelas.

Sehubungan dengan hal tersebut, kami bersyukur dapat menyampaikan rekomendasi kami, dan juga ingin menyampaikan kembali dukungan dan bantuan yang terus kami berikan kepada Pemerintah dalam upayanya untuk mewujudkan perubahan regulasi di Indonesia ini.

Karena itu, di lampiran surat ini, terdapat komentar dan rekomendasi rinci, yang kami ingin KOMINFO pertimbangkan. Selain itu, kami juga menyambut baik kesempatan untuk memberikan masukan dan wawasan kami tentang praktik terbaik industri, secara langsung melalui pertemuan dan diskusi dengan Kominfo serta membantu membentuk dialog untuk kemajuan ekosistem digital di Indonesia.

Jika Anda memiliki pertanyaan atau memerlukan klarifikasi tentang rekomendasi mana pun, jangan ragu untuk menghubungi Sarthak Luthra langsung di Secretariat@aicasia.org atau +65 8739 1490. Terima kasih atas waktu dan pertimbangan Anda.

Hormat kami,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Komentar dan Rekomendasi Detail

Pendahuluan

Asia Internet Coalition (AIC) mendukung pengembangan lingkungan *online* yang aman dan berguna bagi semua pengguna. Sebagai asosiasi industri terkemuka di Asia, kami menangani masalah seperti ekstremisme kekerasan dengan sangat serius dan telah menginvestasikan sumber daya keuangan dan lainnya yang signifikan untuk memberantasnya di seluruh layanan kami, termasuk sistem dan alat untuk mendeteksi dan menanggapi pelanggaran kebijakan dan untuk bertindak atas perintah yang sah untuk hapus konten ilegal. Namun, iterasi terbaru dari peraturan PP 71 - sebagaimana tercermin dalam PM 5 - terus memasukkan dan bahkan menambahkan ketentuan yang mengkhawatirkan tentang konten online yang sensitif dan operator sistem elektronik.

Dalam prosesnya, kami menyesali dan harus menekankan bahwa hanya ada sedikit konsultasi publik dan interaksi menyeluruh dengan pemangku kepentingan terkait sebelum berlakunya keputusan ini. Terlepas dari kenyataan bahwa draf pertama yang diusulkan pada Maret 2020 menimbulkan keprihatinan luas dari berbagai kelompok pemangku kepentingan, dari industri hingga masyarakat sipil, baik secara lokal di Indonesia maupun di luar dari pihak internasional yang berkepentingan. Secara substansi, elemen utama yang dianggap mengkhawatirkan masih ada, dan beberapa aspek tambahan cukup memprihatinkan.

Permasalahan utama

Ruang lingkup dan definisi

PM 5 mencantumkan pasal terkait konten yang dianggap "meresahkan masyarakat dan mengganggu ketertiban umum" sebagai kategori yang dianggap 'mendesak'. Peraturan ini tidak secara jelas mendefinisikan konten seperti apa yang dimaksud. Ketentuan ini juga masih mencakup definisi ambigu dari konten yang dilarang yang dianggap "meresahkan masyarakat" dan "menyediakan cara atau akses ke informasi dan atau dokumen elektronik yang dilarang". Definisi ini menciptakan ruang lingkup yang terlalu luas tentang apa yang dapat dianggap tidak dapat diterima di bawah hukum, dan dengan demikian membuka kemungkinan penegakan yang ambigu dan sewenang-wenang.

Penghapusan konten

Jangka waktu penghapusan juga telah ditentukan menjadi 24 jam, dan untuk konten yang dianggap mendesak, empat jam. Jika tidak ada tindakan yang diambil untuk menghapus konten setelah tiga surat (diberikan dalam jangka waktu 12 jam) denda akan diberikan. Dengan memberikan lebih sedikit waktu bagi PSE Swasta untuk bereaksi, menilai pemberitahuan, dan

mematuhi, terdapat risiko nyata bahwa pemberitahuan oleh pemerintah pada dasarnya merupakan perintah sepihak untuk penghapusan postingan media sosial, tanpa kesempatan untuk dilakukan pengujian. Jika menolak, platform menghadapi risiko nyata diblokir atau menghadapi hukuman finansial yang sangat besar dan tidak proporsional. Hal ini menghadirkan risiko yang jelas terhadap proses hukum dan hak asasi manusia, khususnya kebebasan berekspresi dan informasi. Risiko ini sangat signifikan apalagi siapa pun dapat mengirimkan pemberitahuan penghapusan ke platform, bukan hanya beberapa lembaga yang kompeten (misalnya, Kementerian TIK atau pengadilan).

Draf final dari peraturan ini juga menambahkan kewenangan masyarakat untuk mengajukan permintaan penghapusan konten tentang masalah apa pun - bukan hanya di bidang narkotika, psikotropika, dan perdagangan manusia sesuai draf pertama pada bulan Maret. Hal ini menciptakan potensi cakupan konten yang sangat luas untuk ditargetkan secara tidak proporsional, seperti konten yang dapat dianggap sebagai anti-pemerintah atau ekspresi oleh kelompok minoritas.

Ketentuan wajib untuk mengizinkan pemerintah dan lembaga penegak hukum mengakses PSE Swasta

Elemen lain yang memprihatinkan adalah ketentuan wajib yang memungkinkan pemerintah dan lembaga penegak hukum mengakses sistem dan / atau data elektronik PSE Swasta. Masih belum jelas bagaimana penyediaan akses penegakan hukum akan bekerja dalam praktiknya. Keputusan tersebut sekarang tampaknya memberikan kemampuan yang sangat luas bagi lembaga pemerintah untuk mendapatkan data 'lalu lintas dan pelanggan', tanpa persyaratan yang jelas untuk memberikan alasan hukum, dan kemampuan ini tampaknya akan meluas ke 'lembaga penegak hukum' mana pun, bukan sebatas pada pengadilan. Untuk layanan komputasi awan, prosedur dan mekanisme teknis untuk menyediakan akses ke data juga masih belum jelas. Kewajiban akses data yang ketat ini juga meluas dengan mengkhawatirkan ke sebagian besar perusahaan termasuk startup (lokal), pemain *e-commerce*, media sosial, pengembang *game*. Kewajiban akses data yang luas tersebut selanjutnya menimbulkan pertanyaan yang signifikan terkait dengan hukum dan norma internasional tentang akses data dan aliran data, kebebasan sipil dan kerahasiaan data (yang dapat dianggap sebagai rahasia dagang).

Persyaratan pendaftaran

Peraturan ini mewajibkan PSE Swasta yang didirikan melalui hukum asing atau berada di negara lain untuk mendaftar, jika mereka 1) menyediakan layanan di Indonesia, 2) memiliki bisnis di Indonesia dan / atau 3) memiliki sistem elektronik yang digunakan atau ditawarkan di Indonesia. Hal ini dapat menimbulkan tantangan administratif yang signifikan bagi sejumlah entitas, dan menimbulkan pertanyaan tentang bagaimana hal itu dapat ditegakkan, secara adil dan dengan mempertimbangkan komitmen perdagangan internasional.

Persyaratan apa pun untuk pendirian perusahaan lokal secara paksa dan kehadiran kantor fisik akan berdampak buruk pada investasi langsung asing, pertumbuhan ekonomi, dan pertumbuhan industri TI di Indonesia. Alih-alih memaksa perusahaan untuk membuka kantor lokal, Indonesia

harus mendorong dan memfasilitasi investasi asing melalui insentif, menciptakan lingkungan yang mendukung, dan menumbuhkan basis konsumen yang terhubung ke Internet. Selain itu, keefektifan perusahaan dalam memoderasi konten online tidak bergantung pada keberadaan lokal, melainkan pada proses yang mapan dan kebijakan khusus produk, undang-undang lokal yang jelas untuk memandu proses, dan permintaan penghapusan yang benar dan valid. Persyaratan berat yang diuraikan dalam peraturan yang ada akan menyebabkan konsekuensi yang tidak diinginkan berikut ini:

- *Hambatan non-tarif untuk perdagangan:* Mewajibkan penggabungan lokal dan kehadiran yang tidak perlu mendiskriminasi bisnis asing, menimbulkan hambatan non-tarif untuk perdagangan, dan secara tidak adil mengurangi lapangan bermain untuk mendukung pemain domestik. Ini sangat mencolok mengingat sifat layanan yang disediakan melalui internet, yang dapat diberikan secara lintas batas tanpa perlu kehadiran fisik. Dengan melembagakan persyaratan kehadiran lokal, Indonesia menyimpang dari norma dan praktik perdagangan internasional yang sudah mapan, dan menimbulkan hambatan yang tidak perlu untuk perdagangan jasa lintas batas. Lebih lanjut, jika negara lain membalas dan memberlakukan persyaratan serupa pada bisnis Indonesia, dampak negatif terhadap eksportir IT lokal Indonesia dan industri *freelancing* yang berkembang akan signifikan.

- *Membatasi akses konsumen ke teknologi:* Sifat global Internet telah mendemokratisasi informasi dan membuatnya tersedia untuk siapa saja, di mana saja dalam berbagai bentuk yang tak terbatas. Skala ekonomi yang dicapai melalui infrastruktur yang berlokasi global telah berkontribusi pada keterjangkauan layanan di Internet, di mana beberapa layanan terkemuka tersedia secara gratis. Perusahaan dapat memberikan layanan ini kepada pengguna bahkan di pasar yang mungkin tidak berkelanjutan secara finansial karena mereka tidak perlu mengeluarkan biaya tambahan untuk menyiapkan dan menjalankan kantor lokal dan badan hukum di setiap negara tempat mereka menawarkan layanan. Oleh karena itu, aturan baru ini akan merugikan pengalaman konsumen di Internet terbuka dan meningkatkan biaya.

Singkatnya, kami akan merekomendasikan agar Kominfo mempertimbangkan kembali keputusan tersebut mengingat pertimbangan dan perhatian penting ini, terutama konflik hukum dan tindakan tidak praktis yang akan ditimbulkannya. Kami secara khusus menyarankan agar perbaikan berikut dipertimbangkan oleh kementerian Kominfo.

Rekomendasi

Lingkup penerapan

Ruang lingkup layanan yang diterapkan oleh peraturan harus dibuat dan disesuaikan secara terbatas. Kekhawatiran tentang konten online secara alami harus fokus pada layanan yang dihadapi konsumen yang tujuan utamanya adalah membantu pengguna menyimpan dan menyebarkan konten dengan publik atau khalayak luas lainnya, di mana platform tidak memiliki tanggung jawab editorial - misalnya, jejaring sosial.

Kebebasan berbicara dan berekspresi

Harus ada definisi yang jelas dan dapat ditindaklanjuti tentang apa yang termasuk konten online yang melanggar hukum. Aturan harus mengacu pada ketentuan undang-undang yang spesifik dan substantif untuk definisi tentang apa yang merupakan konten yang melanggar hukum.

Definisi "meresahkan masyarakat" saat ini terlalu luas dan berisiko menghindari peran peradilan (i) dalam menguraikan interpretasi dari rezim hukum fundamental Indonesia dan ketentuan undang-undang yang relevan, dan (ii) untuk mengadili berdasarkan hukum Indonesia. Ini bertentangan dengan asas praduga tidak bersalah.

Waktu penyelesaian tetap untuk memblokir konten

Kerangka waktu yang tepat untuk mematuhi pemberitahuan bukanlah sesuatu yang harus ditetapkan dalam peraturan, karena akan bervariasi dari kasus ke kasus, tergantung pada kerumitan dan volume konten yang sedang dipertimbangkan. Ada juga variasi yang sah antara berbagai teknologi, jenis bisnis, dan konteks.

PSE swasta memerlukan jangka waktu yang wajar untuk menilai permintaan penghapusan setelah semua informasi yang diperlukan telah diberikan oleh individu atau lembaga yang meminta. PSE swasta secara teratur menerima permintaan penghapusan yang terlalu luas, dan analisis pemberitahuan dan permintaan penghapusan di beberapa yurisdiksi menemukan bahwa banyak yang akan mengakibatkan pemblokiran ucapan yang berpotensi sah atau dilindungi.

Dalam banyak kesempatan, PSE Swasta telah menerima permintaan penghapusan yang konon berasal dari sumber pemerintah yang sah, namun ternyata palsu, sehingga membutuhkan uji tuntas dengan niat baik atas permintaan tersebut untuk memvalidasi keabsahannya. Menentukan waktu yang singkat dan spesifik untuk penghapusan atau pemblokiran akan menyebabkan pemblokiran berlebihan pada ucapan yang sah.

Sebaliknya, kami mengusulkan bahwa permintaan harus ditanggapi dalam jangka waktu yang wajar, atau "tanpa penundaan yang tidak semestinya".

Sistem pemberitahuan dapat dilengkapi secara bermanfaat dengan memiliki kejelasan tentang formalitas pengiriman pemberitahuan:

- Identifikasi konten yang dipermasalahkan dengan jelas melalui URL dan jika memungkinkan, sertakan stempel waktu video, atau pengenal unik lainnya (bukan domain tingkat kedua);
- Sebutkan dengan jelas dasar klaim hukum, termasuk ketentuan hukum setempat yang berlaku dan negara tempat hukum tersebut berlaku;
- Identifikasi pengirim pemberitahuan dengan jelas, terutama jika sifat hak yang ditegaskan memerlukan identifikasi pemegang hak; dan
- Membuktikan itikad baik dan validitas klaim menggunakan formulir hukum yang sesuai dengan yurisdiksi (seperti sumpah di bawah hukuman sumpah) dengan hukuman untuk pemberitahuan yang dikeluarkan dengan itikad buruk.

Sistem dan akses data pengguna

Kami menyadari bahwa negara-negara demokratis di seluruh dunia berusaha keras untuk menjaga keamanan warganya. Pemerintah tersebut membutuhkan akses ke bukti digital, yang seringkali dapat dipegang oleh penyedia layanan komunikasi asing.

Peraturan tersebut mengusulkan untuk mengatasi tantangan ini dengan cara yang merusak privasi, keamanan, dan proses hukum bagi pengguna dan dapat menciptakan konflik hukum yang tidak dapat dipertahankan untuk bisnis. Selain itu, persyaratan luas untuk menyediakan akses ke sistem perusahaan tidak dapat dijalankan, mengganggu privasi pengguna, serta kepentingan sah perusahaan.

Sebaliknya, kami mengusulkan untuk bekerja sama untuk mengatasi masalah terkait kerangka kerja bantuan timbal balik yang ada.

Persyaratan pendaftaran

Kami menghargai keprihatinan Anda mengenai keterlibatan lokal dan titik kontak dengan perusahaan asing. Namun, pendekatan yang diusulkan mengancam akan membangun hambatan yang tidak perlu untuk perdagangan jasa lintas batas dan membatasi akses konsumen ke teknologi dan semangat kemudahan berbisnis di Indonesia. Sejauh ada persyaratan untuk koordinasi yang lebih baik antara perusahaan dan regulator, orang yang berdedikasi dapat ditunjuk tanpa persyaratan untuk orang tersebut yang berbasis di daerah.

Batasan penegakan

Penegakan hukum efektif harus berfokus pada kegagalan sistemik dan disengaja saja. Kami menyadari perlunya sanksi yang sesuai untuk kegagalan sistemik perusahaan media sosial dalam

memenuhi permintaan dari pemerintah. Perusahaan media sosial membutuhkan pemahaman yang jelas tentang apa yang dimaksud dengan "kegagalan sistemik" sehingga mereka memiliki jalur yang masuk akal untuk bertindak.

Penilaian kegagalan sistemik harus mempertimbangkan:

- Skala keseluruhan di mana perusahaan media sosial beroperasi;
- Keseluruhan upaya mereka untuk menangani konten bermasalah;
- Risiko untuk melegitimasi pidato dari tindakan tergesa-gesa; dan
- Kebutuhan untuk meluangkan waktu untuk mengarahkan dan memahami masalah baru yang muncul.

Jika dicurigai terjadi kegagalan sistemik, informasi dan / atau pemberitahuan penegakan hukum harus diberikan secara pribadi kepada perusahaan media sosial, memberi perusahaan kesempatan yang wajar untuk menyelidiki, berdiskusi dengan pihak berwenang dan - jika perlu - mengambil tindakan yang sesuai.

Jika masalah yang teridentifikasi terus tidak diperbaiki, maka pihak berwenang harus diizinkan untuk mengeluarkan sanksi yang proporsional untuk kegagalan sistemik. Sanksi ini harus mempertimbangkan skala kegagalan sistemik, dan berhati-hati untuk menghindari insentif yang merugikan bagi perusahaan untuk memblokir konten yang sah guna menghindari hukuman yang berat. Penegakan juga harus memberi perusahaan media sosial kesempatan untuk memberikan klarifikasi, untuk meminta kepatuhan dengan prosedur yang ditetapkan oleh hukum, atau mengajukan banding atas keputusan tersebut kepada pihak berwenang (Kominfo). Sanksi dapat mencakup kemampuan untuk mengeluarkan informasi dan pemberitahuan penegakan, dan untuk "memberi nama dan mempermalukan" platform yang tidak kooperatif dan tidak patuh - dan sebagai upaya terakhir saja, untuk mengenakan denda jika diperlukan.

Komentar dan rekomendasi khusus pasal-pasal

Bab dan Pasal Terkait	Permasalahan	Saran / Rekomendasi
Pasal 2, 3 dan 4 - Persyaratan untuk mendaftar sebagai PSE, termasuk kewajiban untuk mendaftar untuk PSE asing Permintaan pendaftaran juga harus mencakup beberapa dokumentasi tambahan seperti: a. Model bisnis perusahaan; b. Lokasi tempat data dikelola, diproses, dan disimpan; c. Surat Pernyataan dari Private PSE bahwa ia akan memberikan dan memberikan akses ke data dan sistem elektroniknya untuk keperluan pemantauan dan penegakan hukum d. Jumlah pengguna di Indonesia e. Nilai transaksi yang dihasilkan dari Indonesia	Dokumen yang diperlukan untuk pendaftaran mungkin bermasalah untuk diungkapkan, misalnya: nomor pengguna, nilai transaksi, dan data serta pernyataan akses sistem. Tidak ada kejelasan sejauh mana pendaftaran ini menjadikan entitas asing tunduk pada yurisdiksi lokal. Karena pendaftaran ini merupakan prasyarat untuk pendaftaran *e-commerce*, kami mencatat bahwa pendaftaran ini sebenarnya tidak sesuai dengan persyaratan pendaftaran di bawah undang-undang *e-commerce* (PP 80), di mana PM 5/2020 mengharuskan entitas asing untuk mendaftar, sedangkan PP 80 mengharuskan pembentukan entitas lokal.	Persyaratan awal untuk mendaftar yang diatur dalam regulasi sebelum PM 5/2020 sebenarnya jauh lebih fleksibel dibandingkan dengan PM 5/2020. Sarankan untuk menghapus persyaratan dokumen yang bermasalah dan perlu menjelaskan bahwa pendaftaran tidak akan membuat perusahaan asing tunduk pada yurisdiksi lokal.
Pasal 22-31 - Ketentuan Akses ke Kementerian dan Instansi Pemerintah KOMINFO dan Instansi Pemerintah harus memberikan permintaan akses khusus dan kebutuhan untuk memastikan	Kami menemukan bahwa permintaan ini ditafsirkan secara luas, tidak ada definisi yang jelas tentang apa yang dimaksud dengan 'fungsi pengawasan dan pemantauan'. Ada juga jangka waktu 5 hari yang sangat ketat untuk	Harus ada ketentuan yang lebih rinci tentang ruang lingkup fungsi pengawasan dan pemantauan, untuk memastikan bahwa setiap permintaan dapat dibenarkan secara hukum. Perlu juga ditunjukkan bahwa

Bab dan Pasal Terkait	Permasalahan	Saran / Rekomendasi
mekanisme perlindungan terhadap pelanggaran privasi sesuai dengan hukum yang berlaku. Permintaan akses semata-mata untuk tujuan menegakkan fungsi pemantauan dan pengawasan.	menyelesaikan permintaan. Perubahan operasional perlu dilakukan untuk mematuhi jangka waktu Jika akses langsung ke sistem diperlukan, perkakas mungkin perlu dikembangkan untuk digunakan oleh pihak berwenang, yang merupakan beban teknis yang signifikan.	memberikan akses ke data di luar informasi pelanggan dasar (tidak ada data pribadi spesifik yang terlibat) mungkin bertentangan dengan undang-undang AS dan itu akan mempersulit aliran persetujuan internal yang perlu diperoleh platform asing agar sesuai dengan PM 5 / 2020.
Pasal 32-41 - Ketentuan Akses untuk Penegakan Hukum PSE harus menyediakan akses ke data elektronik untuk tujuan menyelidiki pelanggaran pidana, dan terbatas pada pelanggaran tersebut yang memiliki sanksi minimal 2 tahun penjara. Pemberian akses sistem elektronik dibatasi untuk pelanggaran pidana dengan sanksi minimal 5 tahun penjara, atau 2-5 tahun untuk yurisdiksi tertentu yang diputuskan oleh pengadilan negeri setempat. Bagi PSE yang mengelola, mengolah, dan menyimpan data atau sistem elektroniknya di luar negeri, wajib memberikan akses penyelidikan terkait warga negara atau badan usaha Indonesia.	Ada beberapa ketentuan yang bertentangan dengan hukum lain, misalnya hukum AS. Misalnya kewajiban mengungkap konten komunikasi. Ada juga kemungkinan di mana permintaan penegakan hukum tidak sesuai dengan program pengungkapan sukarela yang ada di platform. Menyediakan akses langsung ke sistem akan membuat platform asing menghadapi risiko keamanan yang cukup besar. Ini memperkenalkan titik akhir lain dan sumber kerentanan yang signifikan. Tidak ada visibilitas tentang standar / praktik keamanan siber pemerintah atau malware apa yang mungkin ada di perangkat mereka yang digunakan untuk mengakses sistem. Ada risiko nyata dari akses tidak sah ke sistem platform. Pengguna mereka mungkin menggunakan perangkat yang disusupi (misalnya terinfeksi RAT) yang memungkinkan pihak ketiga yang jahat untuk mengunduh data yang	Harus ada klarifikasi tentang ruang lingkup akses ke sistem yang dipersyaratkan oleh regulasi, dan potensi risikonya. Rekomendasi dan saran yang sama untuk kepentingan Pasal 22-31 di atas.

Bab dan Pasal Terkait	Permasalahan	Saran / Rekomendasi
PSE juga diharuskan menyediakan akses untuk: - Konten Komunikasi, yang dapat didefinisikan sebagai pesan yang dikirim melalui obrolan di platform; dan - Data Pribadi Tertentu, yang mencakup data anak, pandangan politik, dan orientasi seksual.	mereka peroleh dari sistem kami atau mengakses sistem kami tanpa sepengetahuan penggunanya. Jika kasus seperti itu terjadi, platform kemungkinan akan menghadapi pengawasan atas pelanggaran kerahasiaan tersebut, meskipun kerentanan berada di luar sistem kami. Serupa seperti di atas, perubahan operasional dan rekayasa perlu dilakukan untuk menyesuaikan dengan peraturan ini.	
Pasal 9 - Definisi Konten yang dilarang Konten yang dilarang meliputi: a. Konten yang melanggar hukum dan peraturan yang ada b. Konten yang dianggap menyebabkan gangguan publik dan mengganggu ketertiban umum c. Konten yang berisi petunjuk tentang cara mengakses konten terlarang	Kami prihatin definisi yang digariskan dalam kategori (b) akan berimplikasi negatif pada kebebasan berbicara di Indonesia. Cakupan konten yang termasuk dalam kategori (b) tidak didefinisikan secara jelas, khususnya konten yang dapat menimbulkan gangguan publik dan mengganggu ketertiban umum. Agar platform memiliki kepastian yang lebih besar tentang apa yang diperlukan, dan untuk memastikan bahwa undang-undang digunakan dengan cara yang konsisten dengan kebebasan berekspresi, pembatasan ini harus didefinisikan secara jelas dengan parameter dan kriteria.	Harus ada parameter yang jelas dan pedoman tentang: 1. Jenis konten apa yang merupakan konten yang dianggap meresahkan masyarakat dan mengganggu ketertiban umum; 2. Apa kriteria yang digunakan untuk membedakan antara konten yang dianggap meresahkan masyarakat dan mengganggu ketertiban umum "yang diklasifikasikan sebagai permintaan penghapusan"

Bab dan Pasal Terkait	Permasalahan	Saran / Rekomendasi
Pasal 14 - Definisi dari permintaan penghapusan yang "mendesak" Permintaan penghapusan yang mendesak meliputi: a. Terorisme b. Pornografi anak c. Konten yang dianggap meresahkan masyarakat dan mengganggu ketertiban umum	Sebagaimana disebutkan dalam kaitannya dengan Pasal 9, definisi "konten yang dianggap meresahkan masyarakat dan mengganggu ketertiban umum "Tidak didefinisikan dengan jelas. Selain itu, juga tidak jelas kriteria apa yang akan digunakan untuk membedakan antara konten yang dianggap menyebabkan gangguan publik dan mengganggu ketertiban umum ”yang diklasifikasikan sebagai permintaan penghapusan yang“ mendesak ”atau permintaan penghapusan umum.	mendesak "4 jam, dan yang diklasifikasikan dalam permintaan penghapusan 24 jam.
Pasal 15, 16 - Waktu Yang Ketat untuk menanggapi *Take Down Request* (TDR) Permintaan penghapusan konten yang dilarang dalam waktu 24 jam untuk menyelesaikannya Permintaan penghapusan mendesak memiliki waktu 4 jam untuk menyelesaikannya. Namun, peraturan tersebut hanya memberi ruang bagi KOMINFO untuk mempertimbangkan alasan PSE tidak mematuhi jika TDR diterbitkan atas permintaan publik (sedangkan TDR yang dikeluarkan atas permintaan Kementerian / Lembaga, otoritas	Waktu penyelesaian 24 jam dan 4 jam untuk konten mendesak tidak memungkinkan secara operasional. Banyak platform yang sudah memprioritaskan penghapusan konten yang dapat menyebabkan kerusakan dalam waktu dekat. Ada juga konsekuensi yang tidak diinginkan dari sumber daya yang memprioritaskan eskalasi ini daripada menangani konten yang berpotensi lebih berbahaya. Selain itu, memberlakukan jangka waktu 4 jam yang ketat akan mengharuskan platform melanggar norma dan praktik terbaik internasional, dan menghapus konten tanpa bentuk tinjauan apa pun untuk menghindari timbulnya tanggung jawab hukum. Ini akan menyebabkan risiko penegakan berlebih yang sangat tinggi. Undang-undang tidak memberikan jalan bagi pengguna atau PSE	Harus ada proses yang disetujui di mana satu regulator resmi (yaitu KOMINFO) dapat mengirim permintaan penghapusan ke platform. Platform harus diwajibkan untuk: (1) memiliki saluran pelaporan untuk menerima TDR ini, meninjaunya, dan mengambil tindakan yang sesuai (2) memprioritaskan konten yang dapat mengakibatkan bahaya dalam waktu dekat atau yang dapat menyebabkan cedera. Konten semacam itu harus dihapus secepat mungkin (3) ditinjau dan mengambil tindakan pada semua kategori konten lainnya secara tepat waktu. Platform harus diberi

Bab dan Pasal Terkait	Permasalahan	Saran / Rekomendasi
penegak hukum atau lembaga peradilan akan dianggap sebagai tidak perlu dipersoalkan).	untuk menyengketakan keabsahan TDR yang dikeluarkan atas permintaan Kementerian / Lembaga, otoritas penegakan hukum, atau lembaga peradilan. Ketentuan *safe harbour* (Pasal 11) tampaknya memberlakukan kondisi yang memberatkan pada PSE (termasuk melaporkan informasi pelanggan pengguna yang mengupload konten terlarang), sebelum mereka memenuhi syarat untuk *safe harbour*.	waktu yang cukup untuk meninjau konten tersebut dan mengambil tindakan yang sesuai (termasuk pemblokiran geografis, pembatasan gating). TDR yang dikeluarkan atas permintaan Kementerian / Lembaga, otoritas penegak hukum atau lembaga peradilan harus dibenarkan secara hukum (dan tidak dianggap tidak perlu dipersoalkan lagi). Undang-undang harus secara tegas memberikan PSE jalan untuk mengajukan banding / menantang / menyengketakan TDR.

Kesimpulan

Sebagai kesimpulan, PM 5 yang dipublikasikan pada tanggal 2 Desember, selain tidak melalui proses proses konsultasi publik yang layak, menimbulkan sejumlah pertanyaan hukum, ekonomi dan hak asasi manusia yang signifikan, yang dapat berdampak merugikan serius bagi masyarakat dan ekonomi Indonesia, dan perusahaan. prihatin - tanpa benar-benar memberikan cara yang baik untuk menangani masalah konten kontroversial di Internet secara efektif.

AIC dan anggotanya akan sangat mendorong Kominfo untuk mengkaji kembali peraturan ini dan melakukan diskusi mendalam dengan pemangku kepentingan terkait. Sebagai pelaku utama di bidang ini, kami sangat siap dan bersedia mendukung upaya Kominfo untuk menyempurnakan peraturan ini, dan menyukseskan implementasi praktisnya.

<English Translation of this submission is provided from next page onwards>

Detailed comments and recommendations [In English]

A. Introduction

The Asia Internet Coalition (AIC) is supportive of fostering a safe and useful environment online for all users. As a leading industry association in Asia, we take issues like violent extremism extremely seriously and have invested significant financial and other resources to combat it across our services, including systems and tools to detect and respond to violations of policy and to act on valid orders to remove illegal content. Yet, the latest iteration of the regulation GR71 – as reflected in MR5 – continues to include and even add worrisome provisions on sensitive online content and electronic system operators.

On the process, we regret and must emphasise that there has been little if any thorough consultation and interaction with relevant stakeholders ahead of the promulgation of this decree. This is despite the fact that the first draft proposed in March 2020 elicited widespread concern from across stakeholder groups, from industry to civil society, both locally in Indonesia and beyond from interested international parties. On substance, the main elements considered worrisome have remained, and some additional aspects are deeply concerning.

B. Key concerns

Scope and definitions

The revised decree has maintained the concerning clause, which includes content deemed to "instigate public concern and disturbing public order" as a category considered 'urgent'. The regulation does not clearly define what such content would include. It also still includes vaguely worded definitions of prohibited content to include "disturbing public order" and "providing ways or access to information that is prohibited". This represents an overly broad scope of what can be deemed unacceptable under the law, rather than clearly defined as illegal, and it thus opens the possibility of opaque and arbitrary enforcement.

Timeframe for content takedown

The timeframe for takedown has also been specified to 24 hours, and for content deemed urgent, four hours. If no action is taken to take down content after three letters (given over a 12 hours period) a fine will be issued. By providing less time for Private ESOs to react, assess notices, and comply, there is a genuine risk that a notice by the government would in effect constitute a unilateral order for the takedown of social media posts, without the opportunity for due diligence to be properly carried out; otherwise, platforms face the real risk of being blocked or face very large, disproportionate financial penalties. This presents obvious risks to due process and to human rights, in particular freedom of expression and

information. This risk is particularly significant to the extent that anyone may send a platform a removal notice, rather than just a narrow set of qualified authorities (e.g., ICT Ministry, judicial courts).

The latest revision of the regulation also adds the ability for the public to submit content takedown requests on any issues – rather than only in the areas of narcotics, psychotropics and human trafficking as per the first draft in March. This creates the potential for a very broad scope of content to be disproportionately targeted, such as content that could be perceived as anti-government or expressions by minority groups.

Mandatory provision to allow government and law enforcement agencies to access Private ESOs'

Another concerning element is the mandatory provision to allow government and law enforcement agencies to access Private ESOs' electronic systems and/or data. It is still unclear how the law enforcement access provision will work in practice. The decree now seemingly gives a wide-ranging ability for government agencies to obtain 'traffic and subscriber' data, without a clear requirement to provide legal reasoning, and this ability would seem to extend to any 'law enforcement agency', rather than the courts or other duly-appointed judicial authorities. For cloud services, the procedures and technical mechanisms for providing access to data also remain unclear. This strict data access obligation also extends worryingly to a large swathe of companies including (local) startups, e-commerce players, social media, game developers. Such a broad data access obligation further raises significant questions in relation to international law and norms on data access and data flows, civil liberties and data confidentiality (which could be considered as trade secrets).

Registration requirements

The regulation requires Private ESOs which are established through foreign law or reside in other countries to register, if they 1) provide services in Indonesia, 2) have business in Indonesia and/or 3) have electronic systems used or offered in Indonesia. This may present significant administrative challenges for a number of entities, and raises questions as to how it can be enforced, fairly and taking into account international trade commitments.

Any requirement for forced local incorporation and physical office presence will have a deleterious impact on foreign direct investment, economic growth, and Indonesia's growing IT industry. Instead of forcing companies to open local offices, Indonesia should be encouraging and facilitating foreign investment through incentives, creating an enabling environment, and growing the base of Internet connected consumers. Furthermore, the effectiveness with which companies moderate online content does not depend on having local presence, but rather on having well established processes and product-specific policies, clear local laws to guide the process, and properly informed and valid requests for takedowns. The onerous requirements outlined in the existing regulation will lead to the following unintended consequences:

- *Non-tariff barrier to trade:* Requiring local incorporation and presence unnecessarily discriminates against foreign businesses, poses a non-tariff barrier to trade, and unfairly tilts the

playing field in favour of domestic players. This is particularly stark in view of the nature of the services provided through the internet, which can be provided on a cross-border basis without the need for physical presence. By instituting local presence requirements, Indonesia is deviating from established international trade norms and practices, and erecting unnecessary barriers to cross-border services trade. Furthermore, if other countries reciprocate and impose similar requirements on Indonesian businesses, the negative impact on Indonesia's local IT exporters and burgeoning freelancing industry will be significant.

- *Limiting consumer access to technology:* The global nature of the Internet has democratized information and made it available to anyone, anywhere in an infinite variety of forms. The economies of scale achieved through globally located infrastructure have contributed to the affordability of services on the Internet, where several prominent services are available for free. Companies are able to provide these services to users even in markets that may not be financially sustainable as they don't have to incur additional cost of setting up and running local offices and legal entities in each country where they offer services. Therefore, these new rules will harm consumer experience on the open Internet and increase costs.

In summary, we would recommend that Kominfo considers the decree afresh in light of these important considerations and concerns, especially the conflicts of law and impractical measures it would entail. We would suggest in particular the following improvements be considered by the Kominfo ministry.

C. Recommendations

Scope of application

The scope of services to which the regulations apply should be narrowly crafted and tailored. Concerns about online content should naturally focus on consumer-facing services whose principal purpose is helping users store and disseminate content with the public or other broad audiences, over which the platform does not have editorial responsibility -- e.g., social networks.

Freedom of speech and expression (Definitions)

There should be clear and actionable definitions of what constitutes unlawful online content. The Rules should refer to specific and substantive statutory provisions for definitions of what constitutes unlawful content.

The current definition of "public disorder" is overbroad and risks circumventing the role of the judiciary (i) in outlining interpretations of Indonesia's fundamental legal regime and relevant statutory provisions, and (ii) to adjudicate under Indonesian laws. This contradicts the presumption of innocence principle.

Fixed turnaround times for blocking content

The exact time frame for complying with a notice is not something that should be stipulated in the decree, as it will vary from case to case, depending on the complexities and volume of content under consideration. There are also legitimate variations between different technologies, types of businesses, and contexts.

Private PSOs need a reasonable period of time in which to assess the takedown request once all the required information has been provided by the requesting individual or agency. Private PSEs regularly receive overly broad removal requests, and analyses of notice and takedown requests across several jurisdictions have found that many would result in blocking potentially legitimate or protected speech.

On many occasions, Private PSOs have received removal requests that are purportedly from legitimate government sources, but are in fact fake, thus requiring good faith due diligence of the request to validate its legitimacy. Specifying a short and specific time for removal or blocking will lead to overblocking of legitimate speech.

Instead, we propose that requests should be responded to within a reasonable timeframe, or "without undue delay."

The notice system could usefully be complemented by having clarity on the formalities for submitting notices:

- Clearly identify the content at issue by URL and where applicable, include video timestamp, or some other unique identifier (not a second-level domain);
- Clearly state the basis of the legal claim, including the provisions of the applicable local laws and the country in which the law applies;
- Clearly identify the sender of notice, especially where the nature of the rights asserted requires identification of the rightsholder; and
- Attest to the good faith and validity of the claim using the legal form appropriate to the jurisdiction (such as an oath under penalty of perjury) with penalties for notices issued in bad faith.

Systems and user data access

We recognize democratic countries around the world strive to keep their citizens safe. Those governments need access to digital evidence, which can often be held by foreign communication service providers.

The regulation proposes to address this challenge in a way that undermines privacy, security, and due process for users and could create untenable conflicts of law for businesses. Moreover, the broad requirement to provide access to a company's systems is unworkable, invasive of user privacy as well as company's legitimate interests.

Instead, we propose working together to address concerns regarding existing mutual assistance frameworks.

Registration requirements

We appreciate your concerns regarding local engagement and points of contact with foreign companies. However, the proposed approach threatens to erect unnecessary barriers to cross-border services trade and limit consumer access to technology and the spirit of ease of doing business in Indonesia. To the extent there is a requirement for improved coordination between a company and the regulator, a dedicated point person can be appointed without a requirement for the person to be locally based.

Thresholds for enforcement

Effective enforcement should focus on systemic, intentional failures. We recognize the need for appropriate sanctions for a social media company's systemic failure to comply with requests. Then, social media companies need a clear understanding of what constitutes "systemic failure" so they have a reasonable path to action.

An assessment of systemic failure should take into account:

- The overall scale at which social media companies operate;
- Their overall efforts to address problematic content;
- The risks to legitimate speech from precipitous action; and
- The need to take the time to orient to and understand novel issues as they arise.

Where systemic failures are suspected, information and/or enforcement notices should privately be given to a social media company, affording the company a reasonable opportunity to investigate, discuss with the authorities and – if necessary – take appropriate action.

If identified issues continue unrectified, then authorities should be permitted to issue proportionate sanctions for systemic failures. These sanctions should take into account the scale of the systemic failure, and be careful to avoid perverse incentives for companies to block legitimate content to avoid harsh penalties. Enforcement should also afford social media companies the opportunity to provide clarifications, to seek compliance with procedures established by law, or appeal the decision to the authorities (/Kominfo). Sanctions may include the ability to issue information and enforcement notices, and to "name and shame" uncooperative and non-compliant platforms – and as a last resort only, to impose fines where necessary.

D. Article specific comments and recommendations

Related Chapters and Articles	Issues/Reactions	Suggestion/Recommendations
Art 2, 3 and 4 - Requirements for register as Private ESO, including the obligation to register for offshore ESOs The request for registration should also include several additional documentations such as: a. Company business model; b. Location where data are being managed, processed and stored; c. Statement Letter from Private ESO that it will provide and grant access to its data and electronic system for the purposes of monitoring and law enforcement; d. Number of users in Indonesia; and e. Transaction value generated from Indonesia.	The document required for registration may be problematic to disclose, eg: number of users, transaction value, and the data and system access statement. There is no clarity to what extent this registration is subjecting foreign entities to local jurisdiction. As this registration is a prerequisite for e- commerce registration, we note that it is actually inconsistent with the registration requirement under e-commerce law (GR 80), where MR 5/2020 requires an offshore entity to register, while GR 80 requires opening an onshore entity.	The initial requirements to register which are set out in the regulations before MR 5/2020 are actually a lot more flexible compared to MR 5/2020. Suggest removing the problematic document requirements and will need to clarify that registration will not be subjecting foreign companies to local jurisdiction.
Art 22-31 - Provision of Access to Ministries and Government Agencies KOMINFO and Government Agencies should provide a specific request for access and needs to ensure the mechanism of protection against privacy violations in accordance with prevailing laws. The access request is solely for the purpose of enforcing the monitoring and supervisory function.	We found that this request is very broadly interpreted, there is no clear definition of what is meant by 'supervisory and monitoring function'. There is also a very strict timeline of 5 days to complete the request. Operational changes would need to be made to comply with the timeframe If direct access to systems is required, tooling may need to be developed for the authorities to use, which is a significant engineering burden.	There should be a more detailed provision on the scope of supervisory and monitoring function, to ensure that any request can be properly legally justified. Need to also point out that granting access to data outside basic subscriber information (no specific personal data involved) might be in conflict with US laws and that would complicate the internal approval flows that foreign platforms will need to obtain to be in compliance with MR 5/2020.

Related Chapters and Articles	Issues/Reactions	Suggestion/Recommendations
Art 32-41 - Provision of Access for Law Enforcement Private ESOs shall provide access to electronic data for LE for the purpose of investigating criminal violations, and limited to such violations which have a minimum sanction of 2 years imprisonment. Provision of access to electronic system is limited for criminal violations with minimum sanction of 5 years of imprisonment, or 2-5 years for specific jurisdiction as decided by the local district court. For Private ESO that manage, process and store their electronic data or system offshore, it shall provide access for the investigation related to Indonesian citizen or corporate entity. Private ESOs are also required to provide access for: - Communication Content, which could be defined as messages sent over chats in the platform; and - Specific Personal Data, which includes child data, political views and sexual orientation.	There are some provisions which are in conflict with other laws, e.g., US laws. For example, the obligation to disclose communication content. There are also possibilities where a law enforcement request is incompatible with the platform's existing voluntary disclosure program. Providing direct access to systems would expose foreign platforms to considerable security risks. It introduces another end-point and significant source of vulnerabilities. There is no visibility on the government's cybersecurity standards / practices or what malware may be residing on their devices that are used to access the systems. There is a real risk of unauthorized access to the platform's systems. Their users may be utilizing compromised devices (e.g., infected with a RAT) that allows a malicious third party to download the data they obtained from our systems or to access our systems without their users being aware. If such instances occur, platforms will likely face scrutiny for such breaches of confidentiality, even though the vulnerability lies outside our systems.	There should be a clarification on the scope of access to systems that is required by the regulation, and the potential risks. Same recommendation and suggestion to the concerns for Art. 22-31 above.

Related Chapters and Articles	Issues/Reactions	Suggestion/Recommendations
	Similar as above, operational and engineering changes will need to be done to adjust to this regulation.	
Art 9 - Definition of Prohibited Content Prohibited content includes: a. Content that violates existing law and regulation b. Content deemed to cause public disturbance and disrupt public order c. Content that contain instruction on how to access prohibited content	We are concerned that the definition outlined in category (b) will have negative implications for freedom of speech in Indonesia. The scope of content which falls under category (b) is not clearly defined, in particular as to what constitutes content which can cause public disturbance and disrupt public order. In order for platforms to have greater certainty as to what this entails, and to ensure that the law is used in a manner which is consistent with freedom of expression, these restrictions should be clearly defined with parameters and criteria.	There should be clearly defined parameters and guidance on: 1. What type of content would constitute "content deemed to cause public disturbance and disrupt public order; 2. What are the criteria used to differentiate between content deemed to cause public disturbance and disrupt public order" that is classified as an 4 hour "urgent" takedown request, and that classified under 24 hour takedown request.
Art 14 - Definition of "urgent" takedown requests Urgent takedown requests includes: a. Terrorism b. Child pornography c. Content deemed to cause public disturbance and disrupt public order	As mentioned in relation to Article 9, the definition of "content deemed to cause public disturbance and disrupt public order" is not clearly defined. In addition, it is also unclear what are the criteria that would be used to differentiate between content deemed to cause public disturbance and disrupt public order" that is classified as an "urgent" takedown request or general takedown request.	

Related Chapters and Articles	Issues/Reactions	Suggestion/Recommendations
Art 15, 16 - Strict Turnaround Time for government reports Prohibited content takedown requests are on a 24 hour to complete Urgent takedown requests has 4 hours to complete. However, the regulation only gives room for KOMINFO to consider ESO's reason for not complying if the TDR is issued based on a request from the public (whereas TDRs issued on a request from Ministries / Institutions, Law enforcement authorities or judicial institutions would be deemed to be undisputed).	A turnaround time of 24 hours and 4 hours for urgent content is not operationally feasible. Platforms such as FB already prioritize removing content which may cause imminent harm. There are also unintended consequences of resourcing to prioritize these escalations instead of addressing potentially more consequential harmful content. On top of it, imposing a strict 4 hour TAT would require platforms to break with international norms and best practices, and to remove content without any form of review to avoid incurring legal liability. This would lead to an extremely high risk of over-enforcement. The law does not provide for any avenue for a user or ESO to dispute the lawfulness of a TDR issued on a request from Ministries / Institutions, Law enforcement authorities or judicial institutions. The safe harbour provision (Article 11) appears to impose onerous conditions on ESOs (including reporting subscriber information of users who upload prohibited content), before they are eligible for the safe harbour.	There should be an approved process through which one authorized regulator (i.e KOMINFO) is able to send takedown requests to platforms. Platforms should be obliged to: (1) have a reporting channel to receive these TDRs, review them, and take action as appropriate (2) prioritize content which may lead to imminent harm to lives or which may cause injury. Such content should be removed as expeditiously as possible (3) review and take action on all other categories of content in a timely way. Platforms should be permitted sufficient time to review such content and take appropriate action (including geo-blocking, gating restrictions). TDRs issued on a request from Ministries / Institutions, Law enforcement authorities or judicial institutions should be legally justified (and not simply deemed to be undisputed). The law should expressly provide ESOs with avenues to appeal / challenge / dispute TDRs.

E. Conclusion

In conclusion, the Decree as presented on December 2, beside not having benefited from an appropriate consultation process, raises a number of significant legal, economic and human rights questions, which could have serious detrimental impact for Indonesia's people and economy, and the companies concerned - without actually providing a good way forward to tackle effectively the issue of controversial content on the Internet.

AIC and its members would strongly encourage the Kominfo to re-open the legislation and engage immediately in in-depth conversations with relevant stakeholders. As key actors in this area, we stand very ready and willing to support Kominfo's efforts to improve the decree accordingly, and make its practical implementation a success.