USULAN NASKAH AKADEMIK

RANCANGAN PERUBAHAN TERHADAP PERATURAN PEMERINTAH NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK (PP PSTE)



USULAN NASKAH AKADEMIK
RANCANGAN PERUBAHAN TERHADAP PERATURAN PEMERINTAH NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK (PP PSTE)

Tim Penulis
Bramanda Sajiwo
Nurul Izmi



USULAN NASKAH AKADEMIK RANCANGAN PERUBAHAN TERHADAP PERATURAN PEMERINTAH NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK (PP PSTE)

Tim Penulis:
Bramanda Sajiwo
Nurul Izmi

Editor:
Sueb

Layout
Dodi Sanjaya

Ilustrator
Amry Al Mursalaat

Pertama kali dipublikasikan dalam Bahasa Indonesia oleh Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2026

CC BY NC SA

Ringkasan Eksekutif

Dalam lanskap regulasi penyelenggaraan sistem dan transaksi elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) menempati posisi sentral sebagai aturan pelaksana dalam bidang *a quo*. Namun, aturan tersebut dianggap sudah tidak memadai, baik dari aspek yuridis maupun empiris. Secara yuridis, lahirnya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 11/2008 *jo.* UU 1/2024) menuntut penyesuaian mendasar pada level peraturan turunannya. Selain itu, disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU 27/2022) juga mengharuskan PP 71/2019 mengadopsi standar pelindungan data terbaru demi terciptanya sinkronisasi hukum yang utuh. Secara empiris, PP 71/2019 dinilai tidak lagi kompatibel dengan perkembangan PSE saat ini, seperti munculnya beragam layanan, nomenklatur, dan klasifikasi baru sistem elektronik. Selain tertinggal secara teknis, regulasi ini kerap dikaitkan dengan berbagai persoalan di lapangan, mulai dari isu pembatasan kebebasan berekspresi, maraknya kebocoran data pribadi, hingga kendala administratif dalam penyelenggaraan sistem elektronik.

Kajian ini menawarkan arah perubahan PP 71/2019 melalui studi komparasi dengan *good practices* di berbagai negara dan kawasan. Salah satu rujukan utama yang dianalisis adalah Digital Services Act (DSA) dari Uni Eropa, yang merupakan aturan pelengkap khusus bagi *General Data Protection Regulation* (GDPR). Sejumlah ketentuan dalam DSA yang dapat diacu dalam mengubah PP 71/2019 meliputi klasifikasi jenis penyelenggara sistem elektronik berdasarkan skala platform dan jumlah pengguna, tanggung jawab para pihak dalam pelindungan data, transparansi pengelolaan platform, moderasi konten untuk melindungi pengguna dari konten ilegal, hingga pengaturan periklanan digital. Selain Uni Eropa, kajian ini juga mengambil pelajaran dari kerangka regulasi yang

dikembangkan oleh Jepang dan Tiongkok sebagai pembanding di kawasan Asia.

Melengkapi komparasi internasional tersebut, kajian ini turut menganalisis kerangka hukum positif dan arah kebijakan (*ius constituendum*) yang berkaitan berkaitan dengan penyelenggara sistem dan transaksi elektronik di Indonesia. Analisis tersebut menunjukkan bahwa mandat untuk melakukan adaptasi tata kelola sistem elektronik tidak hanya bersumber dari kerangka regulasi sistem dan transaksi elektronik semata, melainkan juga berasal dari berbagai aturan sektoral lainnya. Ketentuan yang mengharuskan adanya penyesuaian tersebut ditemukan pada sektor perdagangan melalui sistem elektronik, pelayanan kesehatan, hingga jurnalisme digital.

Kajian ini menawarkan beberapa solusi strategis berupa sasaran dan arah pengaturan guna merespons perkembangan penyelenggaraan sistem dan transaksi elektronik saat ini. Adapun usulan ruang lingkup perubahan terhadap PP 71/2019 diarahkan pada: (1) definisi dan nomenklatur, guna memuat norma baru terkait perkembangan penyelenggaraan dan transaksi elektronik; (2) pengaturan secara detail dan khusus terhadap mekanisme administratif dalam pendaftaran dan tata kelola penyelenggara sistem elektronik; (3) mengadopsi beberapa *good practices* yang ada di DSA milik Uni Eropa; (4) penambahan bab dan memberikan perhatian pada aktor serta entitas yang terlibat dalam pelindungan data pribadi; (5) memuat pengaturan mengenai pelindungan anak dalam penyelenggaraan sistem elektronik; (6) mengevaluasi dan mengubah sejumlah aturan yang kontroversial dalam PP 71/2019 beserta peraturan teknis turunannya; dan (7) mengakomodasi aturan-aturan sektoral yang berkaitan dengan aspek penyelenggaraan sistem dan transaksi elektronik di Indonesia.

DAFTAR ISI

Ringkasan Eksekutif **i**

DAFTAR ISI **v**

BAB I PENDAHULUAN **3**

A. Latar Belakang **3**

B. Identifikasi Masalah **8**

C. Tujuan dan Kegunaan Penelitian **8**

D. Metodologi Penelitian **9**

BAB II PENYELENGGARA SISTEM ELEKTRONIK: KONSEPTUALISASI DAN PRAKTIKNYA **15**

A. Definisi Penyelenggara Sistem Elektronik **15**

B. Karakteristik Penyelenggara Sistem Elektronik **17**

C. Kategorisasi Penyelenggara Sistem Elektronik **19**

D. Perbandingan Pengaturan terhadap Penyelenggara Sistem Elektronik di Berbagai Negara dan Organisasi Internasional **21**

1. Uni Eropa **21**
2. Tiongkok **32**
3. Jepang **41**

E. Perkembangan Praktik Penyelenggara Sistem Elektronik di Indonesia **62**

BAB III EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN TERKAIT PENYELENGGARAAN SISTEM ELEKTRONIK **71**

A. Peraturan Perundang-undangan Vertikal di atas PP 71/2019 **71**

B. Peraturan Perundang-undangan Horizontal **91**

C. Peraturan Perundang-undangan Vertikal di bawah PP 71/2019 **108**

D. Kebijakan dan Rancangan Peraturan Terkait PP 71/2019 **156**

BAB IV USULAN JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP PENGEMBANGAN PENGATURAN PENYELENGGARA SISTEM ELEKTRONIK **173**

A. Sasaran **173**

B. Arah Pengaturan **173**

C. Jangkauan Pengaturan **174**

D. Ruang Lingkup Materi Pengaturan **175**

BAB V PENUTUP **179**

A. Kesimpulan **179**

B. Rekomendasi **181**

DAFTAR PUSTAKA **183**

BAB I

PENDAHULUAN

BAB I
PENDAHULUAN

A. Latar Belakang

Pengaturan penyelenggaraan sistem dan transaksi elektronik di Indonesia dilandaskan pada ketentuan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019). PP 71/2019 merupakan pengganti dari Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang merupakan aturan derivatif pelaksanaan amanat Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 11/2008) yang telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 1/2024). Subjek pengaturan PP 71/2019 secara garis besar terdiri dari penyelenggara sistem elektronik pada lingkup publik (selanjutnya disebut PSE publik) dan PSE pada lingkup privat (selanjutnya disebut PSE privat).

Substansi PP 71/2019 mengatur kewajiban dan tata teknis penyelenggaraan serta pengelolaan sistem dan transaksi elektronik. Kewajiban PSE dalam PP 71/2019 antara lain: *pertama,* menyediakan sistem elektronik sesuai persyaratan minimum yang dikehendaki oleh PP *a quo*;[1] *kedua,* memastikan sistem elektroniknya tidak memuat serta tidak memfasilitasi penyebarluasan informasi dan/atau dokumen elektronik yang dilarang;[2] *ketiga,* melakukan pendaftaran sistem elektronik sebelum digunakan oleh pengguna;[3] *keempat,* melaksanakan

[1] Pasal 4 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[2] Pasal 5 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[3] Pasal 6 ayat (1) dan ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

prinsip pelindungan data pribadi;[4] *kelima,* melakukan pengelolaan, pemrosesan, dan/atau penyimpanan sistem dan data elektronik di wilayah Indonesia;[5] *keenam,* melakukan pengamanan terhadap sistem elektronik;[6] dan *ketujuh,* mengakomodasi *right to be forgotten* (hak untuk dilupakan) dalam informasi/data elektronik yang sudah tidak relevan. Dari sejumlah kewajiban tersebut, terlihat bahwa materi muatan dalam PP 71/2019 tidak hanya memiliki paradigma pengaturan dalam konteks penyelenggaraan dan pengelolaan sistem elektronik, tapi juga pelindungan data pribadi sebelum diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU 27/2022).

Substansi PP 71/2019 sebetulnya cukup konkret dalam mengatur penyelenggaraan sistem dan transaksi elektronik. Meski demikian regulasi ini masih memiliki sejumlah kelemahan. Kelemahan Pertama terkait dengan pembatasan hak kebebasan berpendapat. PP 71/2019 sebetulnya disusun untuk mencegah peredaran konten ilegal, mengendalikan konten *hoax*, dan memetakan ekosistem transaksi elektronik.[7] Namun, PP 71/2019 sering dikritik karena memberikan celah bagi pemerintah untuk melakukan pembatasan terhadap kebebasan berpendapat di dunia maya dengan berkedok moderasi konten.[8] Celah pembatasan hak kebebasan berpendapat dalam PP 71/2019 terdapat pada ketidakjelasan ruang lingkup Informasi Elektronik (IE) dan/atau

---

4 Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

5 Pasal 20 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

6 Pasal 23 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

7 D. F. Noorhadi, "Pro Kontra Aturan PSE", *Informatika Universitas Islam Indonesia*, https://informatics.uii.ac.id/2022/08/15/pro-kontra-aturan-pse/ (diakses 22 Februari 2026).

8 N. S. M. Sahib. S. Idayanti. K. Rahayu, "Problematika Aturan Penyelenggara Sistem Elektronik (PSE) di Indonesia", *Pancasakti Law Journal*, Vol 1, No. 1 (Juni 2023), 68-69; lihat juga Aliansi Jurnalis Independen, "Serangan terhadap Kebebasan Berekspresi dan Kebebasan Pers Berbahaya Bagi Semua Hak Asasi Manusia Lainnya", AJI Indonesia, https://aji.or.id/informasi/serangan-terhadap-kebebasan-berekspresi-dan-kebebasan-pers-berbahaya-bagi-semua-hak-asasi (diakses 20 Januari 2026).

Dokumen Elektronik (DE) yang melanggar ketentuan peraturan perundang-undangan (*illegal content*) serta meresahkan masyarakat dan mengganggu ketertiban umum (*harmfull content*). Kelemahan kedua berkaitan erat dengan wewenang Pemerintah dalam mencegah gangguan ketertiban umum akibat penyalahgunaan IE dan/atau DE yang diatur dalam UU 1/2024. Dalam undang-undang tersebut, Pemerintah diberikan peran untuk memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik,[9] sekaligus melindungi kepentingan umum dari segala jenis gangguan akibat penyalahgunaannya.[10] Sejalan dengan peran tersebut, Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan IE dan/atau DE yang memiliki muatan dilarang sesuai dengan ketentuan peraturan perundang-undangan.[11] Dalam konteks pencegahan ini, Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada PSE untuk melakukan pemutusan akses.

Ketentuan mengenai kewenangan Pemerintah ini diatur secara derivatif dalam PP 71/2019. Dalam rangka mencegah gangguan ketertiban umum, Pemerintah berperan menetapkan dan mengawasi standar keamanan serta manajemen risiko yang harus dipatuhi oleh penyelenggara. Selain itu, Pemerintah memiliki mandat untuk melakukan pembinaan dan pengawasan terhadap pelindungan infrastruktur informasi vital, termasuk mengoordinasikan langkah-langkah penanganan tanggap darurat.[12] Ketentuan mengenai IE dan/atau DE yang memiliki muatan dilarang mencakup dua aspek utama. *Pertama*, muatan yang secara spesifik melanggar ketentuan peraturan perundang-undangan. *Kedua*, muatan yang dapat meresahkan masyarakat serta mengganggu ketertiban umum. Kedua aspek ini, baik konten yang

[9] Pasal 40 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[10] Pasal 40 ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[11] Pasal 40 ayat (2a) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[12] Pasal 94 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

melanggar peraturan perundang-undangan (*illegal content*) maupun yang meresahkan masyarakat dan mengganggu ketertiban umum (*harmful content*), tidak memiliki pengertian atau batasan yang jelas. Implikasinya, tercipta ketidakpastian hukum pada tataran norma maupun implementasi yang menimbulkan kebingungan bagi PSE Lingkup Publik maupun PSE Lingkup Privat.

Kelemahan ketiga dalam PP 71/2019 adalah kepastian hukum terkait pelindungan data. Ketentuan dalam PP 71/2019 yang berkaitan dengan pelindungan data pribadi perlu dilakukan penyesuaian dan harmonisasi dengan UU 27/2022. Hal ini tidak terlepas dari kedudukan PP 71/2019 yang dinilai publik sebagai produk hukum transisi, dengan tujuan memberikan kepastian pelindungan data pribadi selama pembahasan Rancangan Undang-Undang Pelindungan Data Pribadi (kini UU 27/2022) masih berjalan pada masa tersebut.[13]

Urgensi lain dari diperlukannya perubahan adalah perkembangan dan meningkatnya ancaman siber (*cyberthreat*) serta ekosistem bisnis digital yang juga berkembang dengan cepat. Dalam konteks ancaman siber, Indonesia sendiri telah memiliki preseden berbagai bentuk serangan siber, baik di lingkup publik maupun lingkup privat. Di ranah PSE publik, telah terjadi beragam kasus serangan siber, mulai dari kasus peretasan berupa vandalisme digital atau *defacement,* pencurian data publik seperti data kependudukan dan catatan sipil, hingga penyisipan situs judi daring.[14] Dalam ranah PSE privat juga tidak lebih baik. Berulang kali server dan data PSE privat mengalami pembobolan data pengguna yang kemudian dijual di forum peretas, sebagaimana yang dialami oleh RedDoorz Indonesia dan Tokopedia.

Kelemahan lain dari PP 71/2019 terletak pada nomenklatur dan definisi teknologi yang masih bersifat konvensional. Aturan tersebut membatasi bentuk sistem elektronik hanya pada portal, situs, atau aplikasi, yang tidak lagi relevan

---

[13] V. Rizky, "ELSAM Nilai PP PSTE Hanya Berlaku Sementara", *Jogja Aja,* https://jogjaaja.com/read/elsam-nilai-pp-pste-hanya-berlaku-sementara (diakses 23 Februari 2026).

[14] T. Yuniarto, "Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya", *Kompas,* https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya (diakses 23 Februari 2026).

dengan perkembangan teknologi saat ini. Selain itu, cakupan PSE dalam PP 71/2019 terbatas pada 6 (enam) kategori, yaitu: (1) perdagangan barang dan jasa; (2) transaksi keuangan; (3) pengiriman materi digital; (4) komunikasi; (5) layanan mesin pencari; serta (6) penyediaan informasi elektronik dan pemrosesan data pribadi.[15] Keenam klasifikasi layanan PSE tersebut masih kaku dan terbatas, sehingga perlu diubah agar lebih relevan dengan perkembangan teknologi saat ini seperti: *social commerce, generative artificial intelligence, chatbot artificial intelligence, blockchain,* hingga sistem *Internet of Things*. Belum diaturnya teknologi terkini yang kian ramai digunakan khalayak umum menunjukkan pengaturan PP 71/2019 masih kurang adaptif terhadap perkembangan teknologi yang cepat dan kompleks.

Catatan berikutnya berkaitan dengan tata kelola PSE dalam PP 71/2019 yang belum sepenuhnya disandarkan pada basis hak asasi manusia. Saat ini, terdapat tren global untuk menyesuaikan aturan teknologi dengan standar internasional, seperti ISO dan GDPR. Standar-standar ini telah menjadi acuan umum dalam tata kelola sistem elektronik untuk memberikan kepastian hukum serta menjamin keamanan bisnis dan transaksi elektronik di level internasional.

Revisi terhadap PP 71/2019 merupakan kebutuhan mendesak guna memberikan kepastian hukum yang mampu mewujudkan ekosistem digital Indonesia yang lebih adaptif, aman, dan inklusif. Analisis terhadap PP 71/2019, baik dari sudut pandang normatif maupun empiris, menegaskan bahwa pembaruan komprehensif diperlukan agar regulasi tetap relevan dengan perkembangan teknologi saat ini. Harmonisasi dengan UU 1/2024 dan UU 27/2022 menjadi langkah krusial untuk menjamin kejelasan tata kelola sistem elektronik dan pelindungan data pribadi, sekaligus menciptakan produk hukum yang lebih adaptif terhadap pesatnya perkembangan teknologi.

Penelitian ini akan mengkaji substansi dan implementasi PP 71/2019. Kajian akan menunjukkan sejumlah persoalan dalam penyelenggaraan sistem

[15] Pasal 2 Ayat (3) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

elektronik yang didasarkan pada PP 71/2019. Dengan demikian, kajian ini dapat menjadi landasan untuk mengubah PP 71/2019 sebagai dasar hukum dalam penyelenggaraan sistem dan transaksi elektronik dalam sistem perundang-undangan di Indonesia.

B. Identifikasi Masalah

Berdasarkan uraian di atas, sejumlah masalah yang akan diidentifikasi dalam kajian ini adalah sebagai berikut:

1. Permasalahan apa yang dihadapi dalam tataran normatif maupun implementatif dari PP 71/2019 dalam penyelenggaraan sistem dan transaksi elektronik, serta bagaimana permasalahan tersebut dapat diatasi?
2. Mengapa perubahan terhadap PP 71/2019 diperlukan sebagai dasar pemecahan masalah tersebut?
3. Apa yang menjadi pertimbangan atau landasan filosofis, teoritis, dan empiris dalam pembentukan perubahan terhadap PP 71/2019?
4. Apa sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan dalam perubahan terhadap PP 71/2019?

C. Tujuan dan Kegunaan Penelitian

1. Tujuan
    a. Merumuskan permasalahan yang dihadapi dalam tataran normatif maupun implementatif dari PP 71/2019 dalam penyelenggaraan sistem dan transaksi elektronik, serta bagaimana permasalahan tersebut dapat diatasi;
    b. Merumuskan permasalahan hukum yang dihadapi sebagai landasan pembentukan perubahan PP 71/2019 sebagai dasar

hukum penyelesaian atau solusi permasalahan hukum dalam penyelenggaraan sistem dan transaksi elektronik;

c. Merumuskan pertimbangan atau landasan filosofis, teoritis, dan empiris langkah hukum untuk menyusun perubahan terhadap PP 71/2019;

d. Merumuskan sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan dalam perubahan terhadap PP 71/2019.

2. Kegunaan

Kegunaan penyusunan Naskah Urgensi adalah sebagai acuan atau referensi perubahan PP 71/2019 sebagai dasar hukum penyelesaian atau solusi permasalahan hukum dalam penyelenggaraan sistem dan transaksi elektronik

D. Metode Penelitian

Kajian dalam Naskah Urgensi ini disusun menggunakan kombinasi metode penelitian hukum normatif dan empiris yang dilakukan melalui beberapa tahapan. Pertama, identifikasi dan penetapan masalah yang relevan dengan isu yang diangkat. Kedua, pengumpulan bahan hukum primer, sekunder, dan tersier. Ketiga, analisis terhadap isu hukum berdasarkan seluruh bahan yang telah dikumpulkan guna menjawab permasalahan penelitian.

Dengan menggunakan metode penelitian normatif, kajian ini akan menganalisis konsep, asas, serta prinsip hukum yang relevan bagi perubahan PP 71/2019.[16] Analisis tersebut dilakukan dengan memeriksa sistematika serta keselarasan PP 71/2019 terhadap peraturan perundang-undangan terkait,[17] guna memastikan konsistensi norma. Pelaksanaannya dilakukan melalui kajian

[16] Abdullah Muhammad, *Hukum dan Penelitian Hukum* (Bandung: Citra Aditya Bakti, 2004).
[17] Z. Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2009).

peraturan perundang-undangan terkait teknologi, penyelenggaraan sistem dan transaksi elektronik, serta transformasi regulasi pelindungan data pribadi.

Metode penelitian hukum normatif menjadikan peraturan perundang-undangan sebagai bahan hukum primer. Adapun peraturan perundang-undangan dan rancangan produk hukum yang diacu adalah sebagai berikut:

1. Undang-Undang Nomor 5 Tahun 1999 tentang Persaingan Usaha;
2. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen;
3. Undang-Undang Nomor 40 Tahun 1999 tentang Pers;
4. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran;
5. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
6. Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan;
7. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
8. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik;
9. Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak;
10. Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas;
11. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika

Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat;

12. Peraturan Menteri Perdagangan Nomor 31 Tahun 2023 tentang Perizinan Berusaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan melalui Sistem Elektronik
13. Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik; dan
14. Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Melengkapi pendekatan normatif tersebut, kajian ini juga menggunakan pendekatan penelitian hukum empiris untuk memotret realitas penerapan hukum di lapangan. Pendekatan ini diawali dengan pengolahan data sekunder, yang kemudian diperdalam melalui pengumpulan data primer tentang dampak penerapan sebuah aturan di masyarakat.[18] Melalui pendekatan ini, penyusun dapat melihat kompleksitas dalam penerapan PP 71/2019. Keberadaan penelitian empiris dalam penyusunan kajian ini dilakukan dengan studi kasus empiris yang berkembang serta dokumen hasil penilaian dari pemangku kepentingan dalam sektor terkait. Oleh sebab itu, penelitian ini juga dimaksudkan sebagai perwujudan atas partisipasi masyarakat, khususnya pihak yang terdampak dan terkait dengan pengaturan penyelenggaraan sistem dan transaksi elektronik. Penyusunan dengan model ini telah sejalan dengan ketentuan peraturan perundang-undangan, khususnya Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan sebagaimana telah mengalami perubahan terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang

[18] Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Jakarta: Penerbitan Kencana, 2005).

Perubahan Kedua atas UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (UU 12/2011 *jo.* UU 13/2022).[19]

Selain menggunakan penelitian hukum normatif-empiris, kajian ini juga menggunakan metode perbandingan hukum (*legal comparative study*). Pendekatan ini dilakukan dengan membandingkan hukum yang dikaji dengan hukum yang disusun, ditafsirkan, dan diterapkan di negara lain.[20] Tujuannya tidak hanya untuk memahami norma hukum itu sendiri, tetapi juga bagaimana peran institusi, budaya, bahasa, hingga sejarah hukum dalam mendukung penerapan suatu peraturan di suatu negara.[21]

Fungsi dari perbandingan hukum adalah untuk menemukan praktik dan aturan yang terbaik (*good practices and norms*) dari suatu negara untuk dapat diadopsi dalam hukum negara lain.[22] Wujud perbandingan hukum dalam penelitian ini adalah dengan membandingkan norma, prinsip, dan pemberlakuan suatu peraturan perundang-undangan yang memiliki relevansi dengan penyelenggaraan sistem dan transaksi elektronik.[23] Hal tersebut akan menciptakan suatu analisis kajian perbandingan yang sebanding (*apple-to-apple*), sehingga dapat ditarik konsep dan nilai yang relevan untuk dapat diadopsi dalam revisi terhadap pengaturan penyelenggaraan sistem dan transaksi elektronik di Indonesia.

---

[19] Pasal 96 Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

[20] M. Rheinstein, "Comparative Law - Its Functions, Methods and Usages", *Arkansas Law Review,* Vol. 22, No. 415 (1968), 416-417.

[21] M. Van Hoecke, "Methodology of Comparative Legal Research", *Law and Method,* Vol. 12, No. 1 (2015), 1-6.

[22] *Ibid.*

[23] R. Michaels, "Comparative Law", dalam J. Basedow, K. J. Hopt, *et. al.* (ed.), *Max Planck Encyclopedia of European Private Law* (Oxford: Oxford University Press, 2012), 1–3.

BAB II
PENYELENGGARA SISTEM ELEKTRONIK: KONSEPTUALISASI DAN PRAKTIKNYA

BAB II
PENYELENGGARA SISTEM ELEKTRONIK: KONSEPTUALISASI DAN PRAKTIKNYA

A. Definisi Penyelenggara Sistem Elektronik

Pada era transformasi digital yang terus berkembang, peran teknologi informasi menjadi semakin krusial dalam berbagai aspek kehidupan. Untuk mendukung ekosistem digital yang aman dan andal, maka keberadaan pihak-pihak yang bertanggung jawab dalam penyelenggaraan sistem elektronik menjadi penting dan strategis.[24] Sebutan Penyelenggara Sistem Elektronik (PSE) secara umum mengacu pada pihak-pihak yang berperan penting dalam menyediakan, mengelola, dan mengoperasikan sistem elektronik untuk mendukung berbagai kebutuhan masyarakat, badan usaha, dan pemerintah. Pakar hukum dan teknologi Edmond Makarim mendefinisikan Penyelenggara Sistem Elektronik sebagai berikut:

> *"setiap pihak yang berkontribusi dalam penyelenggaraan suatu sistem elektronik yang mana sistem elektronik sendiri tidak hanya terkait sistem komputer tetapi juga sistem komunikasi, termasuk kecerdasan artifisial."*[25]

Dalam peraturan perundang-undangan definisi PSE pertama kali ditemukan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU 11/2008 Tentang Informasi Dan Transaksi Elektronik (UU 19/2016) *jo* Pasal 1 angka 2 Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016

---

[24] N. Hasan, "Pengaturan *Fintech* dan *Cryptocurrency"*, dalam Fachrurazi (ed.), *Fintech dalam Keuangan Islam: Teori dan Praktik* (Jakarta: Publica Indonesia, 2022), 193.

[25] Disampaikan oleh Edmon Makarim dalam Rapat Dengar Pendapat Umum Komisi I dengan Akademisi/Pakar, sebagaimana termuat dalam Risalah Rapat Dengar Pendapat Umum Komisi I dengan Akademisi/ Pakar di Jakarta, 25 Januari 2023.

tentang Sistem Manajemen Pengamanan Informasi (PM Kominfo 4/2016). Kedua aturan tersebut mendefinisikan PSE sebagai:

> *"Setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain". Definisi ini memberikan gambaran yang jelas tentang cakupan dan peran penyelenggara sistem elektronik dalam mendukung ekosistem digital.*

Berdasarkan definisi tersebut, kegiatan penyelenggara sistem elektronik mencakup tiga aspek utama, yaitu menyediakan, mengelola, dan mengoperasikan sistem elektronik. Ketiga kegiatan ini saling terkait dan bertujuan untuk memastikan keberlanjutan serta efisiensi sistem elektronik yang digunakan oleh berbagai pihak.

Lebih lanjut dalam ketentuan PP 71/2019 juga menyatakan definisi PSE yang serupa, yaitu:

"setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain."

Berdasarkan cakupan yang luas dalam definisi ini, penyelenggara sistem elektronik memiliki berbagai peran penting seperti menyediakan infrastruktur teknologi, mengelola data, dan mengoperasikan platform digital. Tujuan penyelenggaraan sistem elektronik tidak hanya terbatas pada kebutuhan internal penyelenggara, tetapi juga meliputi layanan kepada pihak lain, seperti pengguna individu maupun organisasi.

Definisi PSE dalam regulasi Indonesia menunjukkan ruang lingkup pengertian yang meliputi entitas yang menyediakan, mengelola, dan mengoperasikan sistem elektronik untuk berbagai keperluan. Definisi ini relevan

dengan teknologi terkini seperti *Artificial Intelligence* (AI), *Internet of Things* (IoT), *blockchain*, dan *cloud computing*. PSE yang mengimplementasikan AI dapat mengelola sistem yang memproses data dan membuat keputusan otomatis, seperti asisten virtual atau sistem rekomendasi.

B. Karakteristik Penyelenggara Sistem Elektronik

Definisi PSE dalam PP 71/2019 yang mencakup entitas setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik memberikan dasar hukum yang inklusif terkait siapa dan apa saja peran dari PSE. Jika dijabarkan lebih lanjut, dari definisi tersebut, maka PP *a quo* menjelaskan karakteristik utama PSE merujuk terhadap aktivitas penyediaan, pengelolaan, dan/atau pengoperasian sistem elektronik yang dilakukan oleh setiap entitas tertentu. Adapun wujud dari luasnya ruang lingkup definisi PSE tersebut dapat ditemukan dalam peraturan turunan yang kemudian mengkualifikasikan suatu layanan sistem elektronik sebagai PSE, seperti dalam PM Kominfo 5/2020.

PM Kominfo 5/2020 mengatur mengenai adanya layanan yang dapat dikategorisasi sebagai PSE, misalnya *User Generated Content* dan Komputasi Awan (*Cloud Computing*). Dalam PM Kominfo 5/2020, PSE *User Generated Content* didefinisikan sebagai PSE yang menyelenggarakan aktivitas penyediaan, penayangan, pengunggahan, dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektroniknya dilakukan oleh Pengguna Sistem Elektronik. Selain itu, PSE Komputasi Awan (*Cloud Computing*) yang diatur dalam PM Kominfo 5/2020 adalah PSE yang melaksanakan aktivitas penyediaan, penyelenggaraan, pengelolaan dan/atau pengoperasian model penyediaan akses jaringan yang merata, mudah, berdasarkan permintaan untuk sekumpulan sumber daya komputasi yang dapat dikonfigurasi bersama antara lain jaringan, server, penyimpanan, aplikasi, dan layanan yang dapat disediakan dan dirilis dengan cepat dan dengan daya manajemen atau interaksi penyediaan layanan minimal.

Selain itu, dalam menyelenggarakan aktivitasnya, PSE juga memiliki karakteristik dapat berinteraksi dengan pengguna baik dalam model *Government to Government* (G2G), *Government to Citizen* (G2C), dan *Government to Business* (G2B) dalam PSE Lingkup Publik yang diselenggarakan oleh Instansi,[26] ataupun model *Business to Business* (B2B) dan *Business to Consumer* (B2C) dalam PSE Lingkup Privat.

Status hukum sebagai PSE membawa konsekuensi pada munculnya tanggung jawab tata kelola yang baik dan perlindungan terhadap hak pengguna. Oleh karena itu, PP 71/2019 beserta aturan sektoralnya menetapkan serangkaian kewajiban bagi PSE. Kewajiban PSE di berbagai sektor telah diatur dalam peraturan perundang-undangan sektoralnya masing-masing. Sebagai contoh adalah PSE di bidang keuangan yang telah ditegaskan dalam Pasal 2 ayat (3) Peraturan Otoritas Jasa Keuangan Nomor 41/POJK.04/2020 tentang Pelaksanaan Kegiatan Penawaran Umum Efek Bersifat Ekuitas, Efek Bersifat Utang, Dan/Atau Sukuk Secara Elektronik (POJK 4/2020). POJK 4/2020 menjadi landasan aturan hukum bagi PSE di sektor jasa keuangan untuk menjamin keberlangsungan sistem elektronik melalui berbagai langkah meliputi penyediaan sistem yang berkesinambungan, pengelolaan yang bertanggung jawab, dan penerapan prinsip keamanan yang memadai.

Lebih lanjut, ketentuan Pasal 5 ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik (PM Kominfo 11/2022) menegaskan bahwa pencatatan entitas yang menyelenggarakan sistem elektronik juga merupakan hal yang wajib dilakukan oleh PSE. Pendaftaran ini tidak hanya bertujuan administratif, tetapi juga memastikan bahwa semua PSE dapat diawasi dan dievaluasi oleh pemerintah. Melalui mekanisme pendaftaran, maka pemerintah dapat memastikan bahwa sistem elektronik yang beroperasi di Indonesia memenuhi standar keamanan dan tata kelola yang telah ditetapkan.

---

[26] Lia Muliawaty, Shofwan Hendryawan, "Peranan *E-Government* dalam Pelayanan Publik (Studi Kasus: Mal Pelayanan Publik Kabupaten Sumedang" *Kebijakan: Jurnal Ilmu Administrasi*, Vol. 11, No. 2 (2020), 102.

Kewajiban PSE lainnya adalah menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab, sebagaimana diatur dalam Pasal 3 PP 71/2019. Norma dalam Pasal 3 PP 71/2019 tidak hanya menjadi prinsip dasar, tetapi juga merupakan tolok ukur legalitas suatu PSE yang mengikat. Pemenuhan kewajiban terhadap standar ini menuntut PSE untuk mengambil langkah-langkah proaktif dalam memastikan keamanan data dan stabilitas sistem. Sebab, pelanggaran ketentuan ini dapat membawa konsekuensi berupa tuntutan hukum atau sanksi administratif yang dapat merugikan reputasi atau keberlanjutan operasi PSE.

Kewajiban PSE dalam menyelenggarakan sistem yang aman tidak hanya berhenti pada langkah-langkah proaktif, tetapi juga harus dibuktikan melalui sertifikasi standar sistem manajemen pengamanan informasi sebagaimana ditentukan dalam Pasal 10 ayat (1) PP 71/2019. Sertifikasi tersebut merupakan instrumen penting untuk memastikan bahwa PSE menerapkan praktik terbaik dalam keamanan informasi. Tujuan dari sertifikasi ini tidak hanya menjadi bukti kepatuhan terhadap regulasi, tetapi juga memberikan kepercayaan kepada pengguna sistem elektronik bahwa data mereka dikelola dengan cara yang aman dan bertanggung jawab.

Melalui integrasi karakteristik dan standarisasi kewajiban, terlihat jelas bahwa regulasi ini tidak hanya menitikberatkan pada aspek teknis pengelolaan sistem elektronik, tetapi juga memberikan landasan yang kuat untuk perlindungan hukum bagi semua pihak yang terlibat. Pendekatan komprehensif ini menunjukkan komitmen pemerintah untuk menciptakan ekosistem digital yang aman, terpercaya, dan bertanggung jawab, sekaligus memastikan bahwa Indonesia memiliki infrastruktur hukum yang memadai untuk mendukung transformasi digital.

C. Kategorisasi Penyelenggara Sistem Elektronik

Pemisahan antara PSE lingkup publik dan privat memiliki dasar hukum yang jelas, sebagaimana diatur dalam Pasal 2 ayat (2) dan (3) PP 71/2019. Kedua Pasal *a quo* menyebutkan bahwa PSE terbagi menjadi 2 (dua) yaitu PSE lingkup publik

dan PSE lingkup privat. Klasifikasi ini tidak hanya mendefinisikan cakupan operasional PSE, tetapi juga menentukan tanggung jawab yang melekat pada masing-masing jenis PSE.

PSE lingkup publik adalah penyelenggaraan sistem elektronik oleh instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara, sebagaimana diatur dalam Pasal 2 ayat (3), yang menyatakan bahwa: "*Penyelenggara Sistem Elektronik Lingkup Publik meliputi instansi dan institusi yang ditunjuk oleh instansi tersebut.*" Namun, Pasal 2 ayat (4) menegaskan bahwa kategori ini tidak termasuk PSE lingkup publik yang merupakan otoritas pengatur dan pengawas sektor keuangan.

Ketentuan mengenai PSE lingkup publik dapat dilihat lebih lanjut pada Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik (PM Komdigi 5/2025). PSE Lingkup Publik meliputi instansi dan institusi di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik. Setiap PSE lingkup publik wajib melakukan pendaftaran terhadap sistem elektronik yang diselenggarakannya serta harus menunjuk pejabat pendaftar PSE lingkup publik.

Sementara itu, PSE lingkup privat didefinisikan dalam Pasal 2 ayat (5) PP 71/2019 sebagai penyelenggara sistem elektronik yang diatur atau diawasi oleh kementerian atau lembaga berdasarkan ketentuan peraturan perundang-undangan, serta penyelenggara sistem elektronik yang memiliki portal, situs, atau aplikasi internet untuk menyediakan berbagai layanan yang meliputi:

1. menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau perdagangan barang dan/ atau jasa seperti *Marketplace Tokopedia, Shopee*, dlsb;
2. menyediakan, mengelola, dan/atau mengoperasikan layanan transaksi keuangan seperti PSE yang menyelenggarakan *Internet Banking, Fintech* dompet digital seperti *Dana, Gopay*, serta *Marketplace*;

3. pengiriman materi atau muatan digital berbayar melalui jaringan data baik dengan cara unduh melalui portal atau situs, pengiriman lewat surat elektronik, atau melalui aplikasi lain ke perangkat pengguna seperti Layanan *On-Demand* berbayar;

4. menyediakan, mengelola, dan/atau mengoperasikan layanan komunikasi meliputi namun tidak terbatas pada pesan singkat, panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial seperti *Whatsapp*, *Instagram*, *Telegram*, dlsb;

5. layanan mesin pencari, layanan penyediaan Informasi Elektronik yang berbentuk tulisan, suara, gambar, animasi, musik, video, film, dan permainan atau kombinasi dari sebagian dan/ atau seluruhnya seperti *Search Engine Google*, Layanan Gim, *Netflix*, dll; dan/ atau

6. pemrosesan Data Pribadi untuk kegiatan operasional melayani masyarakat yang terkait dengan aktivitas Transaksi Elektronik seperti Media Sosial dan Platform Komunikasi

D. Perbandingan Pengaturan terhadap Penyelenggara Sistem Elektronik di Berbagai Negara dan Organisasi Internasional

1. Uni Eropa

Pengaturan penyelenggara sistem elektronik (PSE) di Uni Eropa diatur melalui *General Data Protection Regulation* (GDPR), yaitu sebuah regulasi komprehensif yang dirancang untuk melindungi data pribadi sekaligus mendukung pertumbuhan ekonomi digital. GDPR mulai berlaku efektif pada Mei 2018 sebagai landasan utama bagi tata kelola sistem elektronik dalam memastikan pengelolaan data pribadi yang aman, adil, dan transparan di

seluruh negara anggota Uni Eropa.[27] Regulasi ini mengatur PSE yang terlibat dalam pemrosesan data pribadi baik secara langsung maupun melalui pihak ketiga. Berdasarkan konsiderans (*recital*) GDPR, pengaturan ini dirancang untuk menciptakan kepercayaan dalam ekosistem digital, memastikan hak-hak dasar warga negara dilindungi, serta menciptakan arus data yang bebas dan aman di wilayah Uni Eropa.[28]

GDPR memperkenalkan asas-asas yang menjadi pedoman dalam penyelenggaraan sistem elektronik. Salah satu asas utamanya adalah *lawfulness, fairness, and transparency*, sebagaimana diatur dalam Pasal 5 ayat (1) huruf (a), yang berbunyi: "*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*" Tujuan asas ini adalah memberikan jaminan bahwa individu memahami bagaimana data mereka digunakan, serta melindungi mereka dari potensi penyalahgunaan.[29] Asas lainnya adalah *data minimisation*, sebagaimana diatur dalam Pasal 5 ayat (1) huruf (c), yang berbunyi: "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*" Asas ini bertujuan untuk memastikan bahwa hanya data yang relevan dan benar-benar diperlukan yang dikumpulkan dan diproses, sehingga mengurangi risiko kebocoran atau penyalahgunaan data.[30] Selain itu, GDPR juga menetapkan asas *accountability* yang diatur dalam Pasal 5 ayat (2), yang berbunyi: "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*." Maksud dari asas ini adalah untuk menjamin

---

[27] Human Rights Watch, "Peraturan Pelindungan Data Umum Uni Eropa," *Human Rights Watch*, https://www.hrw.org/id/news/2018/06/06/318734 (diakses 11 Februari 2026).

[28] *Vide* Recital No. 4: Data Protection in Balance with Other Fundamental Rights, European Union General Data Protection Regulation.

[29] Information Commissioner's Office, "Principle (a): Lawfulness, Fairness and Transparency," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/ (diakses 11 Februari 2026).

[30] Information Commissioner's Office, "Principle (c): Data Minimisation," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/ (diakses 11 Februari 2026).

agar penyelenggara bertanggung jawab penuh atas semua proses pengelolaan data yang dilakukan dan mampu menunjukkan kepatuhan terhadap GDPR.[31] Kemudian, dalam aspek keamanan, Pasal 32 GDPR menyebutkan bahwa:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."*

Maksud dari pengaturan ketentuan ini adalah agar penyelenggara sistem elektronik mengadopsi langkah-langkah teknis dan organisasi yang memadai untuk melindungi data pribadi dari ancaman, seperti akses tidak sah, kebocoran, atau manipulasi data.[32] Hal ini mencakup penggunaan enkripsi, kontrol akses, dan pengawasan sistem yang rutin. Namun, tantangan terbesar adalah bagaimana menentukan tingkat perlindungan yang "sesuai" dengan risiko, terutama dalam menghadapi serangan siber yang semakin kompleks.[33]

GDPR merupakan regulasi utama Uni Eropa yang menjadi dasar dalam mengatur tata kelola data pribadi oleh PSE. Aturan ini memberikan panduan yang jelas untuk memastikan data pribadi dikelola secara aman, transparan, dan bertanggung jawab, serta melindungi hak individu di era digital. Namun, seiring dengan pesatnya perkembangan teknologi dan ekonomi digital, Uni Eropa menyadari perlunya aturan tambahan untuk mengatur tantangan baru, khususnya di ranah platform digital. Untuk itu, hadir *Digital Services Act* (DSA)

---

[31] Information Commissioner's Office, "Guide to Accountability and Governance," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/ (diakses 11 Februari 2026).

[32] *Vide* Article 32 European Union General Data Protection Regulation.

[33] *Ibid.*

2024 yang melengkapi GDPR dengan fokus pada tanggung jawab penyelenggara sistem elektronik dalam mengelola layanan daring.[34]

DSA 2024 memperkenalkan kewajiban baru berupa transparansi algoritma, pengawasan terhadap moderasi konten, dan perlindungan pengguna dari konten yang ilegal atau berbahaya.[35] Regulasi ini menegaskan peran platform digital untuk lebih bertanggung jawab atas dampak sosial dan hukum dari layanan yang diberikan. Dengan adanya GDPR dan DSA 2024, Uni Eropa tidak hanya berupaya melindungi data pribadi dan privasi individu, tetapi juga menciptakan ruang digital yang aman dan adil bagi semua orang, sambil tetap mendorong inovasi dan pertumbuhan teknologi.

Berbeda dengan dengan GDPR atau regulasi di yurisdiksi lainnya seperti Indonesia, DSA 2024 tidak secara eksplisit membedakan pengaturan antara PSE lingkup publik dan privat. Ketentuan-ketentuan dalam DSA lebih fokus pada jenis layanan digital yang disediakan serta skala operasinya. Pembagian dalam DSA didasarkan pada kategori seperti platform daring yang besar (*Very Large Online Platforms*—VLOPs) dan mesin pencari daring yang besar (*Very Large Online Search Engines*—VLOSEs), yang didefinisikan berdasarkan jumlah pengguna aktif bulanan, yaitu lebih dari 45 juta pengguna di Uni Eropa.[36] Ketentuan ini berlaku untuk semua penyelenggara layanan digital, baik publik maupun privat, selama layanan mereka relevan dengan pengaturan DSA. Hal ini berarti, meskipun secara teknis DSA berlaku untuk kedua lingkup penyelenggara, pengaturannya secara implisit lebih berfokus pada entitas privat yang menjalankan platform digital komersial.

---

[34] European Commission, "Digital Services Act: Questions and Answers," *European Commission Digital Strategy*, https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (diakses 11 Februari 2026).

[35] M. Nidhal, S. Indrayadi, L. Budiman, *et. al.*, "Makalah Kebijakan Nomor 62: Menelusuri Ulasan *Online* di Indonesia: Dampak pada Platform UGC dan Konsumen", 19.

[36] European Commission, "Digital Services Act Starts Applying to All Online Platforms in the EU," European Commission Press Corner, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_881 (diakses 12 Februari 2026).

Kedudukan hukum dari DSA 2024 merupakan regulasi lanjutan yang dirancang untuk melengkapi ketentuan dalam GDPR dengan fokus yang lebih spesifik pada tata kelola platform digital dan penyelenggara sistem elektronik dalam lingkup privat. Ruang lingkup pengaturan DSA tidak hanya melingkupi perlindungan data pribadi, tetapi juga mencakup aspek-aspek baru seperti tanggung jawab transparansi platform, moderasi konten, dan perlindungan pengguna dari konten ilegal atau berbahaya.[37] Salah satu prinsip utama dalam DSA adalah kewajiban bagi penyelenggara sistem elektronik terutama platform daring yang besar untuk bertindak secara transparan terhadap pengguna.[38] Kewajiban transparansi bagi penyelenggara sistem elektronik diatur dalam Pasal 13 DSA, yang menyebutkan bahwa:

> "*Providers of intermediary services shall ensure that terms and conditions are drafted in a clear, accessible, and unambiguous manner and that users are* informed *about the general terms and conditions applicable to their use of the service*".[39]

Ketentuan ini dimaksudkan untuk menjamin bahwa pengguna memahami hak dan kewajiban mereka saat menggunakan layanan platform digital. Ruang lingkupnya mencakup semua penyelenggara yang menawarkan layanan berbasis daring, baik dalam bentuk aplikasi, situs web, maupun platform interaktif lainnya.[40]

---

[37] J.M. Carvalho, F.A. Lima, M. Farinha, "Introduction to the Digital Services Act, Content Moderation and Consumer Protection," *Revista de Direito e Tecnologia*, vol. 3, no. 1 (2021), 71–104.

[38] European Union Agency for Criminal Justice Cooperation, "Digital Services Act – Ensuring a Safe and Accountable Online Environment", *European Union Agency for Criminal Justice Cooperation,*, https://data.europa.eu/doi/10.2812/802073 (diakses 12 Februari 2026).

[39] *Vide* Article 13 Digital Service Act.

[40] European Commission, "The Impact of the Digital Services Act on Digital Platforms," *European Commission Digital Strategy*, https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms (diakses 12 Februari 2026).

Materi muatan dalam DSA turut mengatur kewajiban pencantuman syarat dan ketentuan bagi setiap Penyelenggara Sistem Elektronik. Ketentuan tersebut termuat dalam Pasal 14 DSA, dengan pengaturan sebagai berikut:

1. *Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.*

2. *Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.*

3. *Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.*

4. *Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.*

5. *Providers of very large online platforms and of very large online search engines shall provide recipients of services with a concise, easily-accessible and machine-readable summary of the terms and*

conditions, including the available remedies and redress mechanisms, in clear and unambiguous language.

6. *Very large online platforms and very large online search engines within the meaning of Article 33 shall publish their terms and conditions in the official languages of all the Member States in which they offer their services.*

Pengaturan yang terdapat dalam Pasal/Article 14 dari nomor 1 sampai dengan 6 DSA berkedudukan sebagai dasar dari pemberian kewajiban berimbang khususnya kepada Penyelenggara Sistem Elektronik. Salah satu poin utama dari Pasal *a quo* adalah adanya penindakan dalam moderasi konten, yang mensyaratkan untuk tetap menghormati kebebasan berekspresi para pengguna. Adapun bagi setiap penyelenggara sistem elektronik, terdapat pengecualian tanggung jawab dalam moderasi konten tersebut, selama mereka melakukan upaya penindakan secara responsif melalui penghapusan konten atau pemberian notifikasi

Materi muatan dalam DSA juga mengatur ketentuan mengenai kewajiban moderasi konten dalam Pasal 17 DSA yang menyatakan bahwa:

"Very large online platforms and very large online search engines shall provide for the establishment and implementation of complaint-handling systems and mechanisms for the amicable resolution of disputes."

Maksud dari aturan ini adalah memberikan mekanisme yang jelas dan transparan bagi pengguna untuk melaporkan konten yang dianggap melanggar hukum atau melanggar kebijakan platform.[41] Selain itu, aturan ini bertujuan memastikan bahwa platform bertanggung jawab atas konten yang beredar di dalam sistem mereka, sehingga dapat mencegah penyebaran konten yang merugikan atau ilegal.[42] Namun, salah satu permasalahan yang mungkin

[41] Doris Buijs, "Article 17 Media Freedom Act & the Digital Services Act: Aligned or Alienated?", *DSA Observatory*, https://dsa-observatory.eu/2022/11/25/article-17-media-freedom-act-the-digital-services-act-aligned-or-alienated/ (diakses 12 Februari 2026).

[42] *Ibid.*

muncul adalah beban administratif yang signifikan bagi platform untuk menangani keluhan dalam skala besar, terutama untuk platform yang memiliki jutaan pengguna aktif.

Terdapat pula ketentuan mengenai kewajiban penyusunan laporan tahunan oleh PSE. Ketentuan tersebut diatur dalam Pasal 25 DSA, dengan materi muatan sebagai berikut:

> "*Providers of intermediary services shall publish an annual transparency* report *on the content moderation they undertake, including actions taken to remove or disable access to illegal content and the reasons for such actions*".

Tujuan aturan ini adalah untuk meningkatkan akuntabilitas platform digital dengan memberikan informasi yang jelas kepada publik mengenai mekanisme moderasi konten.[43]

Kewajiban lain yang terdapat dalam Pasal 33 DSA adalah melakukan penilaian (*assesment*) terhadap penyelenggara sistem elektronik yang masuk dalam kategori "*very large online platforms* (*VLOPs*)" atau "*very large online search engines* (*VLOSEs*)". Muatan pasal *a quo* yang memuat kewajiban tersebut, adalah sebagai berikut:

> "*VLOPs and VLOSEs shall conduct risk assessments to identify systemic* risks *stemming from the design, operation, or use of their services and shall implement appropriate mitigation measures*."

Maksud dari pasal ini yaitu untuk menjamin agar platform yang memiliki dampak luas pada masyarakat tidak hanya beroperasi dengan memperhatikan keuntungan, tetapi juga mempertimbangkan dampak sosial, ekonomi, dan keamanan dari layanannya.[44] Ruang lingkup pengaturannya mencakup semua

---

[43] European Commission, "Questions and Answers on the Digital Services Act", *European Commission*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_20_2348/QANDA_20_2348_EN.pdf (diakses 12 Februari 2026).

[44] Magdalena Jóźwiak, "The Wait Is (Almost) Over! First Risk Assessment and Audit Reports – What Will Be Published, When, and the Way Forward," *DSA Observatory*,

platform yang memiliki lebih dari 45 juta pengguna aktif di Uni Eropa.[45] Permasalahan yang sering timbul adalah bagaimana platform dapat secara efektif mengidentifikasi dan mengurangi risiko sistemik, mengingat kompleksitas operasional dan teknologi yang digunakan.

Ketentuan dalam DSA juga mencakup kewajiban perlindungan data pribadi yang spesifik untuk platform digital dengan skala besar, misalnya penggunaan data untuk iklan berbasis perilaku (*behavior based-advertising*). Kewajiban tersebut kemudian berkembang menjadi larangan untuk penggunaan data sensitif untuk tujuan iklan, sebagaimana termaktub dalam ketentuan Pasal 24 DSA, yang menyatakan bahwa:

> "*Providers of intermediary services shall not process personal data of users for the* purpose *of targeted advertising if such data pertain to sensitive categories of personal data*"

Aturan ini bertujuan untuk melindungi privasi pengguna sekaligus mencegah diskriminasi yang mungkin timbul dari penggunaan data sensitif untuk iklan.[46] Namun, tantangan yang dihadapi adalah bagaimana memastikan bahwa penyelenggara benar-benar mematuhi aturan ini, terutama dalam ekosistem digital yang sangat bergantung pada pendapatan dari iklan berbasis data.

Berdasarkan kajian terhadap pengaturan—khususnya dalam hal kewajiban—yang termuat dalam DSA 2024, terlihat bahwa dasar hukum *a quo* memperkuat regulasi penyelenggaraan sistem elektronik di Uni Eropa. Penguatan tersebut diwujudkan dengan materi muatan DSA yang memberikan

---

https://dsa-observatory.eu/2024/11/22/the-wait-is-almost-over-first-risk-assessment-and-audit-reports-what-will-be-published-when-and-the-way-forward/ (diakses 12 Februari 2026).

[45] Redaksi Deutsche Welle Indonesia, "Aturan Baru Uni Eropa untuk Bisnis Digital Mulai Berlaku," *DW.com*, https://www.dw.com/id/aturan-baru-uni-eropa-untuk-bisnis-digital-mulai-berlaku/a-66628099 (diakses 12 Februari 2026).

[46] Amnesty International, "What the EU's Digital Services Act means for human rights and harmful Big Tech business models", *Amnesty Internasional*, https://www.amnesty.org/en/documents/pol30/5830/2022/en/ (diakses 12 Februari 2026).

pengaturan yang lebih rinci dan komprehensif bagi penyelenggara sistem elektronik, khususnya dalam lingkup privat. Regulasi ini menetapkan kewajiban-kewajiban baru yang relevan, seperti transparansi algoritma, moderasi konten, pelarangan penggunaan data sensitif untuk kebutuhan iklan, serta kewajiban penyusunan laporan tahunan tentang moderasi konten. Pengaturan tersebut merupakan respons Uni Eropa terhadap tantangan baru di era digital, seperti meningkatnya ancaman siber dan penggunaan data pribadi yang tidak sesuai aturan. Indonesia juga mengatur penyelenggara sistem elektronik dalam lingkup publik dan privat melalui PP 71/2019, tetapi pengaturan ini dinilai belum sepenuhnya adaptif terhadap perkembangan teknologi dan ancaman yang ada.

Salah satu hal yang dapat dipelajari dari DSA adalah komitmen Uni Eropa dalam menciptakan ekosistem digital yang aman dengan aturan yang ketat mengenai transparansi algoritma dan pelindungan data. Pengaturan seperti ini penting untuk diadopsi di Indonesia, terutama dalam konteks larangan penggunaan data pribadi untuk kebutuhan iklan berbasis algoritma tanpa persetujuan eksplisit, seperti yang diatur dalam Pasal 24 DSA. Hal tersebut relevan mengingat isu penggunaan data pribadi di Indonesia masih menjadi persoalan, baik dalam lingkup publik maupun privat. Kondisi ini kian mendesak untuk ditangani, mengingat terdapat sejumlah kasus peretasan dan pembobolan data yang melibatkan PSE privat seperti yang dialami Tokopedia dan RedDoorz.[47] Peristiwa-peristiwa tersebut menunjukkan perlunya regulasi yang lebih kuat di Indonesia dalam menjamin keamanan data dan mencegah penyalahgunaan.

Materi muatan dalam DSA juga dapat menjadi acuan dalam menyusun pengaturan yang lebih jelas mengenai kewajiban PSE privat untuk melaporkan moderasi konten dan dampaknya terhadap pengguna. Dalam konteks PP 71/2019, aturan terkait moderasi konten masih prolematik karena dinilai dapat

[47] Tenri Gobel, "RedDoorz Alami Kebocoran Data, Pelanggan Diminta Ganti Password," *Cyberthreat.id*, https://cyberthreat.id/read/8614/RedDoorz-Alami-Kebocoran-Data-Pelanggan-Diminta-Ganti-Password (diakses 12 Februari 2026).

menjadi alat untuk membatasi kebebasan berpendapat di dunia maya. Sementara itu dalam Pasal 25 DSA—yang mengatur kewajiban penyelenggara untuk menyusun laporan tahunan transparansi—dapat dijadikan referensi untuk memastikan akuntabilitas PSE di Indonesia tanpa mengorbankan hak-hak kebebasan digital masyarakat.

Tidak hanya itu, poin lain yang dapat diambil dari DSA adalah ketentuan Pasal 14 DSA. Dalam hal tersebut, terdapat ketentuan mengenai pembagian tanggung jawab dalam kewajiban penindakan sebagai tindak lanjut dalam moderasi konten. Materi dalam DSA dapat diadopsi oleh Indonesia dalam merevisi PP 71/2019, khususnya untuk mengatur kedudukan dan pertanggungjawaban dalam penanganan konten ilegal sebagai bagian dari moderasi konten.

Selain itu, ketentuan Pasal 33 DSA juga dapat diadopsi, di mana platform digital besar diwajibkan untuk melakukan penilaian risiko sistemik sebagai bentuk mitigasi dalam penyelenggaraan sistem elektronik. Muatan tersebut sangat relevan bagi Indonesia, mengingat tingkat ancaman siber yang tinggi dan banyaknya serangan terhadap PSE publik maupun privat. Revisi terhadap PP 71/2019 perlu memperhatikan kewajiban ini untuk menjamin bahwa PSE memiliki mekanisme pencegahan risiko yang memadai—terutama bila berkaca terhadap ancaman siber seperti *ransomware* yang pernah melumpuhkan Pusat Data Nasional Indonesia pada 2024.

Harmonisasi pengaturan antara PP 71/2019 dengan prinsip-prinsip dalam DSA juga dapat membantu Indonesia mengembangkan regulasi yang lebih sesuai dengan kebutuhan industri digital yang berkembang pesat. Ketentuan dalam DSA menunjukkan bahwa pengaturan yang adaptif dan berbasis risiko dapat memberikan jaminan lebih baik bagi perlindungan pengguna, meningkatkan kepercayaan terhadap ekosistem digital, serta memberikan kepastian hukum bagi pelaku usaha. Dengan mengadopsi norma ketentuan dari DSA, Indonesia dapat lebih siap menghadapi tantangan era digital dengan tetap

menjaga keamanan siber, melindungi data pribadi, dan memastikan ruang digital yang adil bagi semua pihak.

2. Tiongkok

Lanskap perlindungan data di Tiongkok telah mengalami transformasi signifikan selama beberapa tahun terakhir, yang mencerminkan semakin diakuinya masalah privasi di negara tersebut. Secara historis, Tiongkok tidak memiliki undang-undang perlindungan data yang komprehensif. Hal ini menyebabkan pengaturan yang ada bersifat fragmentaris, sehingga memicu inkonsistensi dan ketidakpastian hukum dalam perlindungan data pribadi.[48] Namun, seiring berkembangnya ekonomi digital dan semakin pentingnya internet dalam kehidupan sehari-hari, kebutuhan akan pendekatan terstruktur terhadap perlindungan data semakin jelas. Dalam beberapa tahun terakhir, insiden pelanggaran data dan penyalahgunaan informasi pribadi telah mendorong seruan dari masyarakat dan pemerintah untuk perlindungan yang lebih kuat.[49] Salah satu momen penting dalam sejarah perlindungan data Tiongkok adalah pemberlakuan *Cybersecurity Law* (CSL) yang menjadi dasar bagi peraturan selanjutnya dengan membahas komponen utama keamanan data dan perlindungan informasi pribadi.[50]

Kerangka hukum penyelenggaraan sistem elektronik di Tiongkok diatur melalui tiga udang-undang, yakni CSL, *Data Security Law* (DSL), dan *Personal Information Protection Law* (PIPL).[51] Ketiga undang-undang ini mengatur keamanan siber, pengelolaan data, dan perlindungan informasi pribadi yang

---

[48] T. Kawase, "Understanding the Chinese Data Security Law: Explaining the Measures Japanese Companies Should Take," *Monolith Law*, https://monolith.law/en/general-corporate/china-data-security-law (diakses 14 Februari 2026).

[49] *Ibid.*

[50] Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity*, vol. 8, No. 1 (2022), 1-12.

[51] R.D. Junck, B.A. Klein, A Kumaki, *et. al.*, "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies," *Skadden Arps, Slate Meagher & Flom LLP*, https://www.skadden.com/-/media/files/publications/2021/11/chinas_new_data_security_and_personal_information_protection_laws_what_they_mean.pdf?rev=271e4258db3d4a02845addffb7ae4b1c (diakses 14 Februari 2026).

saling melengkapi. CSL mulai berlaku pada tahun 2017 dan berlaku untuk semua operator jaringan, pemilik jaringan, operator, dan penyedia layanan di Tiongkok.[52] Pasal 1 CSL menyebutkan bahwa,

> *"This Law is formulated for the purposes of protecting cybersecurity, safeguarding cyberspace sovereignty, national security and public interests, protecting the lawful rights and interests of citizens, legal persons, and other organizations, and promoting the sound development of economic and social informatization".*

Tujuan utama CSL sebagaimana ditegaskan dalam Pasal *a quo* adalah melindungi keamanan siber dan kedaulatan ruang siber, serta menjaga keamanan nasional dan kepentingan publik.[53] Dengan pengaturan ini, pemerintah berupaya untuk menciptakan lingkungan digital yang aman dan terkendali, memberikan kepastian hukum bagi warga negara dan entitas bisnis, serta mendorong transformasi digital yang bertanggung jawab.

Selanjutnya, Pasal 2 CSL mengatur mengenai ruang lingkup pemberlakuan aturan PSE, dengan menyebutkan bahwa,

> *"This Law shall apply to the construction, operation, maintenance, and use of networks as well as the supervision and* administration *of cybersecurity within the territory of the People's Republic of China".*

Pasal ini menetapkan cakupan hukum yang luas, mencakup semua aktivitas yang terkait dengan jaringan dalam wilayah Tiongkok. Artinya semua

---

[52] Martina Gerst, "China's New Cyber Security Law: What It is About and How to Prepare for It", *EU SME Centre*, https://www.eusmecentre.org.cn/publications/chinas-new-cyber-security-law-what-it-is-about-and-how-to-prepare-for-it/ (diakses 14 Februari 2026).

[53] PriceWaterhouseCoopers, "A Comparison of Cybersecurity Regulations: China," *PwC*, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html (diakses 14 Februari 2026).

penyelenggara jaringan, baik domestik maupun asing, harus mematuhi regulasi ini jika beroperasi di Tiongkok.[54]

CSL juga mengatur ketentuan mengenai sistem perlindungan bertingkat. Ketentuan ini diatur pada Pasal 21 CSL yang menyebutkan bahwa,

> *"The State shall implement a multi-level cybersecurity protection system. Network operators shall perform the following security protection duties according to the requirements of the multi-level cybersecurity protection system to ensure that networks are free from interference, damage, or unauthorized access, and prevent network data from being disclosed, stolen, or falsified."*

Ketentuan mengenai *Multi-Level Protection Scheme* (MLPS) ini memberikan kewajiban kepada operator jaringan untuk mengambil langkah-langkah teknis dan manajerial dalam menjaga keamanan jaringan.[55] Undang-undang ini berfokus pada perlindungan keamanan data internet yang mewajibkan operator jaringan untuk menerapkan langkah-langkah keamanan yang diperlukan guna melindungi informasi pengguna.[56]

Selain itu, CSL menetapkan standar untuk lokalisasi data sehingga data penting yang dihasilkan di dalam wilayah Tiongkok wajib disimpan di dalam negeri.[57] Hal ini diatur dalam Pasal 37 CSL yang menyebutkan bahwa,

---

[54] C. Bigg, A. Ge, *et. al.*, "CHINA: Enhanced and Clarified Data Compliance Obligations on Handlers of 'Network Data', Covering Personal Information and Important Data, and Operators of Online Platforms from 1 January 2025," *Privacy Matters by DLA Piper*, https://privacymatters.dlapiper.com/2024/10/china-enhanced-and-clarified-data-compliance-obligations-on-handlers-of-network-data-covering-personal-information-and-important-data-and-operators-of-online-platforms-from-1-january-2025/ (diakses 14 Februari 2026).

[55] Reed Smith, "MLPS 2.0: China's Enhanced Data Security Multi-Level Protection Scheme and Related Enforcement Updates," *Reed Smith*, https://www.reedsmith.com/en/perspectives/2019/10/mlps-20-chinas-enhanced-data-security-multi-level-protection (diakses 14 Februari 2026).

[56] *Ibid.*

[57] O. Sun, "Cross-Border Data Transfer Mechanism in China and Its Compliance," *California Lawyers Association*, https://calawyers.org/business-law/cross-border-data-transfer-mechanism-in-china-and-its-compliance/ (diakses 15 Februari 2026).

"Operators of critical information infrastructure that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China shall store such information/data within Mainland China. If, due to business requirements, it is necessary to provide such information/data outside of the territory of Mainland China, a security assessment shall be conducted".

Ketentuan ini dirancang untuk melindungi data strategis dari potensi penyalahgunaan oleh pihak luar, namun secara bersamaan ketentuan ini dapat menjadi tantangan bagi perusahaan internasional yang beroperasi di Tiongkok.[58] Ketentuan ini mencerminkan strategi yang lebih luas dari pemerintah Tiongkok untuk mempertahankan kendali atas data dan memperkuat keamanan nasional.[59] Selain itu, CSL juga mengatur perlindungan *Critical Information Infrastructure* (CII) melalui langkah-langkah keamanan khusus.[60] Selain itu, undang-undang ini juga mengatur ketentuan mengenai kewajiban keamanan siber bagi operator jaringan dan *Critical Information Infrastructure Operator* (CIIO) di Tiongkok.[61]

Tiongkok tidak membedakan operator informasi publik dengan privat pada peraturan yang dimiliki. Namun, pada praktiknya informasi yang berkaitan dengan energi, transportasi, pelayanan air, kesehatan publik, dan *e-government* dikelola oleh entitas publik seperti instansi pemerintah, badan usaha milik negara, rumah sakit pemerintah, dan lembaga-lembaga lain yang beroperasi di sektor layanan publik.[62] Namun, terdapat pula CII yang dikelola oleh sektor privat, misalnya layanan komunikasi dan informasi publik yang dikelola oleh penyedia

---

[58] C. Zhang, "China's Privacy Protection Strategy and Its Geopolitical Implications," *Asian Review of Political Economy*, vol. 3, no. 6 (2024), 5-11.

[59] *Ibid.*

[60] *Ibid.*

[61] *Ibid.*

[62] Z. Zhang, "A Close Reading of China's New Cybersecurity Review Measures, in Effect Feb 15, 2022," *China Briefing*, https://www.china-briefing.com/news/a-close-reading-of-chinas-new-cybersecurity-review-measures-in-effect-february-15-2022/ (diakses 15 Februari 2026).

jaringan telekomunikasi dan layanan *cloud*, layanan keuangan yang dikelola oleh bank komersial, dan *platform* digital yang dikelola oleh *e-commerce.*

Tiongkok telah memiliki CSL sebagai regulasi yang mengatur ketentuan mengenai keamanan data, namun regulasi tersebut masih bersifat umum dan belum terfokus pada kerangka tata kelola keamanan data.[63] Mengatasi persoalan tersebut Tiongkok kemudian membentuk DSL yang disahkan pada musim panas 2021 dan berlaku mulai pada tanggal 1 September.[64] Peraturan ini diundangkan hampir empat tahun setelah berlakunya CSL pada 2017, sebuah regulasi yang mengategorikan dan mengatur pengelolaan data di Tiongkok. Berbeda dengan CSL yang lebih umum dan berfokus pada keamanan jaringan serta infrastruktur kritis, DSL menawarkan pendekatan yang lebih terstruktur dalam penanganan data dengan memperkenalkan klasifikasi yang jelas dan kewajiban perlindungan yang spesifik.[65]

Dalam DSL, data dikategorikan menjadi data biasa, data penting, dan data inti. Setiap kategori tersebut memerlukan tingkat perlindungan yang berbeda sesuai dengan sensitivitas dan dampaknya terhadap keamanan nasional, kepentingan publik, atau hak individu.[66] Ketentuan ini berlaku untuk semua aktivitas pemrosesan data, baik daring maupun luring. Pengundangan DSL bertujuan untuk memastikan potensi risiko keamanan data dapat dimitigasi,

---

[63] J. Gong, "The Data Security Law of China ('DSL'), Together with the Personal Information Protection Law of China ('PIPL')," *Bird & Bird*, https://www.twobirds.com/en/trending-topics/china-privacy-and-data-protection (diakses 15 Februari 2026).

[64] *Ibid.*

[65] A. Kokas, "China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges," *China Leadership Monitor* 70, https://www.prcleader.org/post/china-s-2021-data-security-law-grand-data-strategy-with-looming-implementation-challenges (diakses 15 Februari 2026).

[66] D.L. Cohen, T.R. Savio, J. Jiang, *et. al*, "Impact of the New China Data Security Law for International Investors and Businesses," *Akin Gump Alerts*, https://www.akingump.com/en/insights/alerts/impact-of-the-new-china-data-security-law-for-businesses-and-international-investors-1 (diakses 15 Februari 2026).

sekaligus melindungi data yang berkaitan dengan kepentingan nasional dan publik.[67]

DSL berlaku tidak hanya untuk aktivitas pemrosesan data di dalam wilayah Tiongkok, tetapi juga meluas ke aktivitas di luar negeri yang dapat mengancam keamanan nasional, kepentingan publik, atau hak-hak warga Tiongkok.[68] Penerapan ekstrateritorial ini menegaskan niat Tiongkok untuk mengawasi transaksi data internasional yang melibatkan kepentingan negara. Salah satu fitur unik DSL adalah kewajiban untuk menyusun katalog nasional data penting.[69] Katalog ini dikelola oleh otoritas pusat dan regional.[70] Katalog ini berfungsi sebagai panduan bagi industri untuk mengidentifikasi jenis data yang dikelola dan menerapkan langkah-langkah perlindungan yang sesuai.[71]

DSL juga mewajibkan para pengolah data yang menangani kategori data penting untuk melakukan penilaian risiko secara berkala.[72] Penilaian ini bertujuan mengidentifikasi kerentanan potensial dan menyampaikan laporan hasilnya kepada otoritas pemerintah terkait.[73] Untuk mekanisme transfer data lintas batas, undang-undang ini menerapkan tinjauan keamanan yang ketat untuk memastikan bahwa data yang ditransfer keluar dari Tiongkok tidak

---

[67] InCountry Staff, "China's Digital Data Sovereignty Laws and Regulations," *InCountry Blog,* https://incountry.com/blog/chinas-digital-data-sovereignty-laws-and-regulations/ (diakses 16 Februari 2026).

[68] G. Kennedy, J. W. J. Lai, J. Wong, "PRC Network Data Security Management Regulations," *Mayer Brown Publications,* https://www.mayerbrown.com/en/insights/publications/2024/12/prc-network-data-security-management-regulations (diakses 20 Februari 2026).

[69] G. Interesse, "China Issues New Regulations on Network Data Security Management, Effective January 1, 2025," *China Briefing,* https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/ (diakses 20 Februari 2026).

[70] *Ibid.*

[71] *Ibid.*

[72] S. Ning, H. Wu, "Cybersecurity 2022: China Law & Practice and China Trends & Development," *Chambers Global Practice Guides,* https://www.kwm.com/content/dam/kwm/insights/download-publication/china/2023/Chambers%20Cybersecurity%202022.pdf (diakses 15 Februari 2026).

[73] *Ibid.*

membahayakan kepentingan nasional.[74] Transfer informasi kritis terutama data inti diawasi secara ketat untuk mencegah penyalahgunaan atau akses yang tidak sah.

Dalam perkembangannya, Cybersecurity Administration of China (CAC)—selaku otoritas keamanan siber di Republik Rakyat Tiongkok, menerbitkan beberapa peraturan yang mendukung pelaksanaan regulasi mengenai platform digital di Tiongkok. Salah satu kasus yang sedang marak adalah penyalahgunaan data pribadi untuk algoritma media sosial dan *e-commerce.* Merespons situasi tersebut, CAC menerbitkan *Administrative Provisions on Algorithmic Recommendation for Internet Information Services/*互联网信息服务算法推荐管理定 (Administrative Provisions) yang mulai berlaku sejak 1 Maret 2022.[75] Peraturan ini mengatur kewajiban bagi PSE untuk mengungkapkan penyedia layanan untuk mengungkapkan prinsip kerja utama algoritma platform dan menjamin algoritma tidak digunakan untuk memanipulasi opini publik atau menyebarkan informasi yang melanggar ketentuan hukum.[76] Hal ini diatur pada Pasal 14 Administrative Provisions yang menyebutkan bahwa,

> *"Algorithm recommendation service providers shall not falsely register accounts, illegally trade accounts, manipulate user accounts or make false likes, comments or forwarding by taking advantage of algorithms, nor shall they block information, overly recommend, manipulate lists or search results ranking, control the most searched or selections by taking advantage of algorithms to intervene in information presentation or to have*

---

[74] B. Li, "China's New Cross-Border Data Transfer Regulations: What You Need to Know and Do," *IAPP News,* https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do (diakses 21 Februari 2026).

[75] Bird & Bird, "Data as a Key Digital Asset: China – Data and Evolving Digital Regulation: Algorithm Regulation," *Bird & Bir*d, https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/apac-dra/apac-dsd/data-as-a-key-digital-asset/china/data-and-evolving-digital-regulation-algorithm-regulation (diakses 21 Februari 2026).

[76] *Ibid.*

any act of influencing network public opinions or circumventing supervision and administration".

Melalui ketentuan ini, Pemerintah Tiongkok berupaya menciptakan transparansi, menjamin keadilan sosial, dan melindungi privasi serta hak pengguna layanan dalam ekosistem digital.

Kemudian, Pasal 12 Administrative Provisions juga menyebutkan bahwa:

"Algorithmic recommendation service providers shall comprehensively use tactics such as content de-weighting, scattering interventions, etc., and optimize the transparency and understandability of search, ranking, selection, push notification, display, and other such norms, to avoid creating harmful influence on users, or triggering controversies or disputes"

Melalui ketentuan ini, Pemerintah Tiongkok berupaya untuk mencegah terjadinya penggunaan algoritma untuk diskriminasi harga berdasarkan data pengguna seperti memberikan harga yang berbeda kepada pengguna untuk produk atau layanan yang sama.[77]

Selanjutnya, Pasal 15 Administrative Provisions juga menyebutkan bahwa,

"Algorithmic recommendation service providers shall provide users with a choice to not target their individual characteristics, or provide users with a convenient option to switch off algorithmic recommendation services, the algorithmic recommendation service provider shall immediately cease providing related services.

Algorithmic recommendation service providers shall provide users with functions to choose, revise, or delete user tags used for algorithmic recommendation services.

[77] R. Zeng, X. Li, "On the Illegality and Regulation of Algorithmic Price Discrimination in China's Digital Economy," *Journal of Politics and Law*, vol. 16, no. 4 (2023):13-19.

Where users believe algorithmic recommendation service providers use algorithms in a manner creating a major in the algorithmic recommendation service provider to give an explanation and adopt related measures to improve or remedy the situation."

Adanya ketentuan ini kemudian membawa makna bagi pengguna layanan dapat memilih untuk keluar dari personalisasi algoritma sehingga pengguna layanan dapat menggunakan layanan digital tanpa rekomendasi yang berbasis data pribadi.

Indonesia dapat belajar banyak dari pengalaman Tiongkok dalam mengatur PSE dan pelindungan data pribadi. Tiongkok telah menerapkan regulasi yang komprehensif melalui CSL, DSL, dan PIPL. Ketiga regulasi ini merupakan regulasi yang saling melengkapi dalam menjaga keamanan data, melindungi hak pengguna, dan mendukung transformasi digital yang inklusif. Selain itu, Tiongkok juga telah membuat peraturan khusus untuk mengatur penggunaan algoritma melalui *Administrative Provisions on Algorithmic Reccomendation for Internet Information Services.*

Berdasarkan perbandingan dengan Tiongkok, maka Indonesia dapat menerapkan pendekatan yang serupa dengan melakukan perubahan terhadap PP 71/2019. Indonesia juga perlu untuk membuat peraturan mengenai algoritma untuk memastikan agar algoritma tidak disalahgunakan, baik untuk manipulasi opini publik maupun diskriminasi harga berdasarkan data pribadi. Selain itu, Indonesia juga perlu mendorong transparansi dalam pengelolaan data oleh PSE dan memberikan hak yang lebih besar kepada pengguna untuk mengontrol data pribadi pengguna. Langkah ini dapat dilakukan dengan mengatur ketentuan agar pengguna memiliki opsi untuk keluar dari layanan berbasis algoritma.

Kerja sama antara pemerintah, sektor swasta, dan lembaga akademik juga perlu ditingkatkan untuk menyusun katalog data penting dan melakukan penilaian risiko secara berkala. Indonesia juga harus memperkuat pengawasan dan penegakan hukum melalui BSSN dan juga Kementerian Komunikasi dan

Digital (Komdigi) yang memiliki kapasitas untuk menjamin kepatuhan PSE terhadap regulasi. Dengan belajar dari pengalaman Tiongkok, Indonesia dapat menciptakan sistem regulasi yang mendukung keamanan data dan privasi pengguna tanpa menghambat pertumbuhan ekonomi digital.

3. Jepang

Act on the Protection of Personal Information (APPI) merupakan salah satu regulasi terpenting dalam tata kelola data pribadi di Jepang. APPI diterapkan pertama kali pada 2005 dan telah mengalami amandemen pada 2017 dan 2020.[78] APPI bertujuan untuk memberikan perlindungan data pribadi di tengah pesatnya perkembangan teknologi digital dan globalisasi data. Regulasi ini mengatur kewajiban PSE dalam mengumpulkan, memproses, menyimpan, dan mentransfer data pribadi, termasuk pengaturan terkait data lintas batas yang semakin krusial di era digital. APPI juga memberikan hak kepada individu untuk mengakses, mengoreksi, dan meminta penghapusan data pribadinya, sekaligus mendorong transparansi dalam praktik pengelolaan data oleh perusahaan. Dengan semakin kompleksnya ekosistem digital, APPI berfungsi sebagai kerangka hukum yang fleksibel namun ketat, menjadikan Jepang sebagai salah satu negara dengan standar perlindungan data yang setara dengan Peraturan Perlindungan Data Umum (GDPR) Uni Eropa.

Dalam APPI terdapat perbedaan yang jelas antara Penyelenggara Sistem Elektronik (PSE) publik dan privat. Perbedaan ini diatur dalam Article 2 Paragraph (5) APPI, yang mendefinisikan bahwa:

> *"a personal information handling business operator means a person providing a personal information database etc. for use in business; however, excluding a central government organization, a local government,*

[78] K. Takase, D. Tatsuno, "Japan Enacts Amendments to the Act on the Protection of Personal Information," *Baker McKenzie InsightPlus*, https://insightplus.bakermckenzie.com/bm/investigations-compliance-ethics/japan-enacts-amendments-to-the-act-on-the-protection-of-personal-information (diakses 23 Februari 2026).

an incorporated administrative agency etc., or a local incorporated administrative agency".

Berdasarkan ketentuan ini, PSE publik meliputi pemerintah pusat, pemerintah daerah, serta badan administrasi terinkorporasi yang berfungsi mengelola data untuk layanan publik dan administrasi. Sebaliknya, PSE privat mencakup entitas bisnis yang mengelola data untuk keperluan komersial.

Lebih lanjut, Article 8 hingga Article 13 APPI mengatur langkah-langkah perlindungan data oleh pemerintah pusat dan daerah. Pasal 8 menyatakan bahwa:

> *"The central government shall provide information, develop guidelines to ensure the proper and effective implementation of action to be taken by a business operator etc., and take other necessary action in order to support measures for the protection of personal information developed or implemented by a local government and activities undertaken by a Japanese citizen, or a business operator etc. in relation to seeking the proper handling of personal information".*

Maksud dari pengaturan ini adalah untuk memberikan kepastian hukum bahwa pemerintah pusat mengambil peran aktif dalam memberikan arahan dan dukungan kepada pemerintah daerah, pelaku usaha, maupun warga negara terkait perlindungan data pribadi. Dengan ini, pemerintah pusat berfungsi sebagai pengarah utama dalam pengelolaan data yang aman dan sesuai hukum.

Sementara itu, Article 9 APPI berkaitan dengan langkah masuknya pemerintah dalam penyelesaian sengketa terhadap PSE, dengan menyebutkan bahwa:

> *"The central government shall take necessary action to seek the proper and prompt dealing of a complaint caused between a business operator and a principal about the handling of personal information."*

Ketentuan ini bertujuan untuk menjamin bahwa keluhan yang muncul antara individu dan pelaku usaha terkait pengelolaan data pribadi dapat diselesaikan secara tepat dan cepat. Hal ini menunjukkan pentingnya peran pemerintah dalam memediasi konflik demi melindungi hak individu.

Sedangkan ketentuan mengenai peran pemerintah daerah diatur dalam Article 11 APPI yang menyebutkan bahwa,

> *"A local government shall, considering the nature of personal information it retains, the purpose of retaining the personal information, and so on, strive to take necessary action so as to ensure the proper handling of the retained personal information."*

Maksud dari Pasal *a quo* adalah untuk mendorong pemerintah daerah mengambil langkah-langkah yang diperlukan untuk memastikan bahwa data pribadi yang dikelolanya diproses dengan tepat, sesuai dengan tujuan penyimpanan data tersebut. Hal ini menegaskan pentingnya pengelolaan data yang kontekstual dan bertanggung jawab di tingkat daerah yang dijabarkan lebih lanjut hingga Pasal 13 APPI.

Pembagian tanggung jawab serta langkah teknis dalam APPI mengakomodasi karakteristik dan fungsi spesifik setiap sektor. Pendekatan ini bertujuan memastikan pengelolaan data pribadi dilakukan secara efektif dan adil bagi masyarakat, baik di tingkat pusat maupun daerah.

Selain mengatur PSE privat, APPI juga menetapkan kewajiban bagi PSE publik. Entitas privat yang meliputi perusahaan atau organisasi bisnis, memiliki tanggung jawab besar dalam mengelola data pribadi terutama karena sifat operasionalnya yang berorientasi pada kepentingan komersial. Ketentuan ini bertujuan untuk menciptakan ekosistem bisnis yang transparan, bertanggung jawab, dan selaras dengan hak privasi individu. Rincian tanggung jawab PSE privat dalam APPI dapat dilihat pada tabel di bawah ini:

Tabel 2. 1. Pemetaan Tanggung Jawab PSE Privat dalam APPI

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
Article 15 Paragraph (1)	*"A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a "utilization purpose") as explicitly as possible."*	Memastikan transparansi dengan mewajibkan pelaku usaha menentukan tujuan penggunaan data secara jelas sejak awal, sehingga mengurangi risiko penyalahgunaan data pribadi.
Article 16	*"A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article."*	Membatasi penggunaan data di luar tujuan awal tanpa persetujuan individu, dengan pengecualian tertentu seperti keselamatan publik atau kewajiban hukum, untuk melindungi privasi individu.
Article 20	*"A personal information handling business operator shall take necessary and appropriate action for the*	Mewajibkan pelaku usaha menerapkan langkah-langkah pengamanan untuk melindungi data dari

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	security control of personal data including preventing the leakage, loss or damage of its handled personal data."	kebocoran, kehilangan, atau kerusakan, sehingga meningkatkan kepercayaan masyarakat terhadap pengelolaan data.
Article 23 ayat (1)	*A personal information handling business operator shall, except in those cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent.* *i. cases based on laws and regulations* *ii. cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent* *iii. cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to*	Mengatur batasan ketat dalam pemberian data kepada pihak ketiga, sehingga menjamin individu tetap memiliki kendali atas data pribadinya. Pengecualian yang diatur mencakup kepentingan hukum, keselamatan publik, dan kerja sama dengan pemerintah.

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	obtain a principal's consent *iv. cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs*	
Article 27 Paragraph (1)	*A personal information handling business operator shall, concerning its retained personal information, put those matters set forth in the following into a state where a principal can know (including those cases in which it, at the request of a*	Memberikan hak kepada individu untuk mengetahui secara transparan bagaimana data pribadi mereka dikelola, termasuk nama dan alamat pengelola data, tujuan penggunaan data, prosedur pengajuan permintaan terkait data, serta

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	principal, responds without delay). *(i). the name or appellation and address and, for a corporate body, the name of its representative of the said personal information handling business operator* *(ii). the utilization purpose of all retained personal data (excluding those cases falling under item (i) through item (iii) of Article 18, paragraph (4))* *(iii). the procedures for responding to a request pursuant to the provisions of the succeeding paragraph, or, a demand pursuant to the provisions of the succeeding Article, paragraph (1) (including as applied mutatis mutandis pursuant to the succeeding Article, paragraph (5)); Article 29, paragraph (1); or Article 30, paragraph (1),*	informasi penting lain yang dijamin oleh undang-undang.

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	paragraph (3) or paragraph (5) (including, when the amount of a fee has been decided pursuant to the provisions of Article 33, paragraph (2), the amount of the fee) *(iv). besides those set forth under the preceding three items, those prescribed by cabinet order as a necessary matter to ensure the proper handling of retained personal data.*	
Article 28	*A principal may demand of a personal information handling business operator disclosure of retained personal data that can identify him or herself by a method of providing electromagnetic record or other methods prescribed by rules of the Personal Information Protection Commission.*	Memberikan hak akses kepada individu terhadap data pribadinya sehingga individu dapat memantau, mengoreksi, atau menghapus data jika diperlukan. Hal ini bertujuan untuk memperkuat kontrol individu terhadap informasi pribadinya.

Sumber: diolah Penulis (2026).

Seluruh ketentuan yang diatur dalam APPI menunjukkan bahwa Jepang memiliki komitmen kuat untuk menciptakan ekosistem perlindungan data pribadi yang komprehensif. Regulasi ini membagi tanggung jawab secara jelas antara PSE publik dan privat serta memberikan hak kepada individu untuk mengontrol data pribadinya. Ketentuan-ketentuan dalam APPI tidak hanya menjamin keamanan data tetapi juga memberikan landasan hukum yang kuat untuk menjaga transparansi dan kepercayaan dalam pengelolaan informasi. Menanggapi ekosistem digital yang kompleks, APPI hadir sebagai regulasi adaptif yang memenuhi kebutuhan masyarakat modern serta menjawab tantangan global pelindungan data pribadi.

Jauh sebelum APPI berlaku, Jepang telah memiliki regulasi pelindungan data dan privasi khusus sektor komunikasi, yaitu *Telecommunications Business Act* (TBA) atau Act No. 86 of December 25, 1984. Undang-undang ini ditetapkan untuk merespons perkembangan sektor telekomunikasi yang mengalami kemajuan pesat akibat adopsi teknologi komunikasi mutakhir pada masa itu.[79] Setelah diberlakukan pada tahun 1985, TBA telah mengalami beberapa kali perubahan guna menyesuaikan dengan kemajuan teknologi dan tantangan baru yang dihadapi. Amandemen terbaru TBA mulai berlaku pada 16 Juni 2023. Amandemen TBA memperkenalkan sejumlah ketentuan penting yang berfokus pada perlindungan data pengguna dan pengelolaan informasi dalam sektor telekomunikasi yaitu pengaturan khusus mengenai pengiriman informasi ke pihak ketiga.[80]

---

[79] Y. Arai, "History of the Development of Telecommunications Infrastructure in Japan," *Netcom*), https://journals.openedition.org/netcom/4511, https://doi.org/10.4000/netcom.4511 (diakses 23 Februari 2026).

[80] Data Guidance JP, "Japan: Amendments to Telecommunications Business Act Enter into Effect," *Data Guidance,* https://www.dataguidance.com/news/japan-amendments-telecommunications-business-act-enter (diakses 23 Februari 2026).

Salah satu ketentuan utama dalam amandemen ini adalah terkait definisi *Information Transmission Command Communications* yang rumuskan sebagai:[81]

> *"transmission of telecommunications that commands a user's telecommunications facilities in which information about the user is recorded, to transmit to telecommunications facilities other than the user."*

Ketentuan ini mencakup pengiriman data dari perangkat pengguna seperti komputer atau ponsel pintar, ke fasilitas telekomunikasi lain, termasuk server pihak ketiga.[82] Pengaturan ini bertujuan untuk menjamin transparansi dalam pengelolaan data, memberikan kontrol yang lebih besar kepada pengguna, dan melindungi privasi individu.

Berbeda dengan APPI, TBA tidak secara eksplisit membedakan antara PSE publik dan privat. Fokus utama TBA adalah pada jenis layanan telekomunikasi yang disediakan dan dampaknya terhadap pengguna sebagaimana diatur dalam Article 2 Paragraph 2 TBA. Ketentuan ini mendefinisikan *"telecommunications business"* sebagai:

> *"the business involved in providing telecommunications services in order to meet the demands of other persons (except businesses involved in service supplying facilities for broadcasting stations as prescribed in Article 118, paragraph (1) of the Broadcasting Act (Act No. 132 of 1950))"*

Ketentuan tersebut memperlihatkan bahwa rezim aturan Jepang tidak membedakan apakah layanan tersebut dikelola oleh entitas publik atau privat. Amandemen terbaru pada TBA memperluas cakupan regulasi untuk mencakup bisnis yang sebelumnya dikecualikan (*Exempted Businesses*). Semua penyedia layanan telekomunikasi yang memiliki dampak signifikan pada pengguna, seperti layanan email, platform media sosial, layanan *streaming*, dan e-

---

[81] T. Hollwarth, "New Cookie Regulations in Japan – Amendment of Telecommunications Business Act," *EuroCloud News*, https://www.eurocloud.at/news/detail/news/new-cookie-regulations-in-japan-amendment-of-telecommunications-business-act/ (diakses 23 Februari 2026).

[82] *Ibid.*

commerce kini berada dalam pengawasan regulasi.[83] Perubahan ini menunjukkan bahwa TBA kini menitikberatkan pada skala layanan dan dampaknya terhadap pengguna, sehingga setiap entitas yang memiliki pengaruh besar wajib mematuhi ketentuan yang berlaku tanpa memandang status organisasinya.[84]

Penegakan regulasi TBA berada di bawah tanggung jawab *Ministry of Internal Affairs and Communications* (MIC) Jepang. MIC memiliki wewenang untuk mengawasi kepatuhan bisnis telekomunikasi, yang diatur dalam berbagai ketentuan dalam TBA. Salah satu wewenang penting MIC diatur dalam Article 29 Paragraph (1) TBA yang menyatakan bahwa,

> *"If the Minister for Internal Affairs and Communications finds that a telecommunications carrier falls under any of the following items, the Minister may order the telecommunications carrier to improve its means of conducting the operations or take other measures to the extent necessary for ensuring the interests of users or the public interest".*

Ketentuan ini memberikan MIC kewenangan untuk memerintahkan perbaikan operasional atau tindakan lain terhadap penyelenggara telekomunikasi jika ditemukan kegiatan usaha yang merugikan kepentingan pengguna atau publik, termasuk ketidakpatuhan terhadap kerahasiaan komunikasi atau syarat layanan yang tidak pantas.[85]

Selanjutnya, Article 65 TBA mengatur mengenai kewajiban kepatuhan terhadap TBA, dengan menyebutkan bahwa,

> *"If a notifying supplier has fulfilled its obligation pursuant to the provisions of the preceding Article with regard to the specified terminal equipment based on the design subject to notification, it may affix the*

---

83 *Ibid.*

84 *Ibid.*

85 Ministry of Internal Affairs and Communications, "Report on Telecommunications Policy,"*Ministry of Internal Affairs and Communications*, https://www.soumu.go.jp/main_content/000979390.pdf (diakses 24 Februari 2026).

marks specified by Order of the Ministry of Internal Affairs and Communications on the specified terminal equipment."

Ketentuan ini memberikan kewenangan kepada MIC untuk mengatur dan menyetujui tanda kepatuhan pada peralatan telekomunikasi sebagai bukti bahwa perangkat tersebut telah memenuhi standar desain yang ditetapkan. Melalui ketentuan ini, MIC menjadi lembaga yang bertanggung jawab dalam menjamin kepatuhan penyelenggara telekomunikasi terhadap standar teknis dan operasional yang berlaku. Dengan prinsip dan kewajiban yang diatur secara rinci, TBA bertujuan melindungi kepentingan pengguna dengan meningkatkan transparansi, memberdayakan kontrol data individu, dan memitigasi risiko penyalahgunaan data dalam sektor telekomunikasi.

Selain APPI dan TBA, Jepang juga memiliki kerangka hukum lain yang memperkuat perlindungan data dan keamanan digital, yaitu *Basic Act on Cybersecurity* (BAC). Regulasi ini disahkan pada 12 November 2014 untuk menetapkan kebijakan keamanan siber yang komprehensif di Jepang.[86] BAC bertujuan menjamin keamanan infrastruktur digital negara dengan memastikan aliran informasi yang aman, mencegah ancaman siber, dan membangun ketahanan terhadap potensi kerusakan akibat serangan siber.[87] Salah satu komponen penting dari undang-undang ini adalah pembentukan *Cybersecurity Strategic Headquarters*, yang bertanggung jawab untuk merumuskan dan melaksanakan strategi keamanan siber nasional, mengawasi kebijakan yang dijalankan oleh kementerian dan lembaga terkait, serta memfasilitasi koordinasi antara sektor publik dan privat dalam menghadapi ancaman siber.[88]

Pada tahun 2018, undang-undang ini diamendemen untuk memperkuat langkah-langkah keamanan menjelang Olimpiade dan Paralimpiade Tokyo

[86] Article 1-Purpose, Japanese Basic Act on the Protection of Personal Information.
[87] The Government of Japan, *Japan Cybersecurity Strategy* (Tokyo: The Government of Japan, 2015), 1-2
[88] *Ibid.*

2020.[89] Amandemen tersebut mencakup pembentukan *Council for Cybersecurity Measures* yang melibatkan pemerintah, operator infrastruktur informasi kritis, dan institusi pendidikan dan penelitian, serta mendelegasikan sebagian fungsi *Cybersecurity Strategic Headquarters* kepada entitas seperti *Information-Technology Promotion Agency* (IPA) dalam hal penetapan standar keamanan siber dan pelaksanaan audit keamanan.[90] Dengan adanya produk hukum BAC, Jepang memperkuat posisinya dalam menghadapi tantangan teknologi modern dan berperan aktif dalam kerja sama internasional untuk keamanan digital global. Undang-undang ini melengkapi APPI dan TBA, menciptakan kerangka hukum yang komprehensif untuk melindungi data dan infrastruktur digital Jepang di era modern.

BAC menetapkan prinsip-prinsip dasar serta tanggung jawab yang komprehensif untuk menangani ancaman keamanan siber yang terus berkembang, baik secara domestik maupun internasional. Sebagaimana dijelaskan dalam Article 3 BAC, yaitu,

> *"...the promotion of the Cybersecurity policy must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders, including the national government, local governments, and critical information infrastructure (CII) operators,.."*

Pasal ini menunjukkan bahwa dalam menegakkan regulasi ini diperlukan kolaborasi antara pemerintah pusat, pemerintah daerah, operator infrastruktur informasi kritis, dan masyarakat untuk menciptakan sistem yang tangguh dalam menghadapi ancaman siber.[91]

---

[89] U. Sayuri, "Japan: Basic Act on Cybersecurity Amended," *Global Legal Monitor, Library of Congress*, https://www.loc.gov/item/global-legal-monitor/2018-12-26/japan-basic-act-on-cybersecurity-amended/ (diakses 24 Februari 2026).

[90] *Ibid.*

[91] Hiromi Hayashi, Masaki Yukawa, and Daisuke Tsuta, "Cybersecurity Laws and Regulations: Japan 2025," *ICLG - Cybersecurity Laws and Regulations*, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan (diakses 24 Februari 2026).

Terdapat pembagian tanggung jawab antara pemerintah pusat dan daerah dalam mengelola keamanan siber di Jepang.[92] Tanggung jawab utama pemerintah nasional dalam menjamin keamanan siber diatur dalam Article 4 BAC, yang menyatakan bahwa, *"...the national government bears the responsibility to formulate and implement comprehensive cybersecurity policies".* Kemudian, Article 12 BAC juga menyebutkan bahwa:

> "*The national government must establish a basic plan for Cybersecurity (hereinafter referred to as the "Cybersecurity Strategy") with the aim of the comprehensive and effective promotion of the Cybersecurity policy*".

Ketentuan ini memberikan tanggung jawab kepada pemerintah nasional untuk menetapkan strategi keamanan siber di Jepang.

Di sisi lain, pemerintah daerah juga memiliki tanggung jawab tersendiri sebagaimana dijelaskan dalam Article 5 BAC, yang berbunyi,

> *"In accordance with the Basic Principles, local governments bear the responsibility to formulate and implement independent* Cybersecurity *policies in consideration of the appropriate division of roles with the national government."*

Ketentuan ini menunjukkan pentingnya pembagian tanggung jawab antara pemerintah pusat dan daerah, di mana kebijakan di tingkat daerah harus sejalan dengan strategi nasional, namun tetap memperhatikan kebutuhan daerah.

Sementara itu, operator infrastruktur informasi kritis (*Critical Information Infrastructure Operators*) memiliki kewajiban penting sebagaimana diatur dalam Article 6 BAC, yang menyatakan:

> *"CII Operators shall deepen their awareness and understanding of the critical value of cybersecurity, ensure cybersecurity voluntarily and*

[92] *Ibid.*

proactively, and cooperate with measures on cybersecurity taken by the national government or local governments".

BAC juga menjelaskan mekanisme koordinasi antara pemerintah daerah dengan *Cybersecurity Strategic Headquarters*. Ketentuan tersebut diatur dalam Article 32 BAC, yang menyebutkan bahwa:

> *"(1) Local governments may request the provision of information and other cooperation from the Headquarters where necessary, for the establishment and implementation of the policies prescribed under Article 5.*
>
> *(2) When cooperation is requested pursuant to the preceding paragraph, the Headquarters are to make an effort to meet the request."*

Ketentuan ini memperkuat hubungan antara pemerintah daerah dan pusat melalui koordinasi yang lebih baik. Pemerintah daerah diberi kewenangan untuk meminta bantuan secara langsung dari *Headquarters* yang diwajibkan untuk merespons permintaan tersebut dengan upaya terbaiknya. Hal ini merupakan upaya untuk memastikan agar kebijakan pemerintah daerah tetap selaras dengan strategi nasional namun tetap menyesuaikan kebutuhan spesifik daerah.

Lebih lanjut, penegakan BAC berada di bawah pengawasan *Cybersecurity Strategic Headquarters*, sebagaimana dijelaskan dalam Article 24 BAC, yang berbunyi,

> *"For the purpose of effectively and comprehensively promoting Cybersecurity policies, the Cybersecurity Strategic Headquarters (hereinafter referred to as the 'Headquarters') are to be established under the Cabinet".*

Pasal 24 BAC mengamanatkan pembentukan *Cybersecurity Strategic Headquarters* di bawah Kantor Kabinet sebagai badan utama yang bertanggung jawab atas pelaksanaan kebijakan keamanan siber. Pembentukan

markas besar ini bertujuan untuk menyediakan koordinasi lintas sektoral yang terpusat, baik di tingkat nasional maupun daerah dalam merespons ancaman keamanan siber yang semakin kompleks.

Keberadaan lembaga ini juga memperkuat struktur kelembagaan Jepang untuk menjawab tantangan siber global melalui pendekatan yang terkoordinasi. Untuk mendukung pelaksanaan fungsinya, sejumlah ketentuan dalam BAC menjelaskan wewenang dan tanggung jawab Headquarters secara rinci. Tabel berikut merangkum letak norma, materi muatan, serta maksud dan tujuan dari pasal-pasal yang mengatur peran dan fungsi Headquarters dalam mengelola keamanan siber di Jepang:

Tabel 2. 2. Pemetaan Pasal dalam BAC yang Mengatur Mengenai Tugas, Fungsi, dan Kewenangan Headquarters dalam Mengelola Keamanan Siber di Jepang.

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
Article 25	*"(1) The Headquarters will carry out the following functions:* *(i) Preparing the Cybersecurity Strategy and promoting it implementation.* *(ii) Establishing the standards of Cybersecurity measures for national administrative organs and Incorporated Administrative Agencies, and promoting the implementation of the evaluation (including audit) of measures based on the standards and*	Mengatur fungsi utama Headquarters seperti menyusun strategi keamanan siber, menetapkan standar langkah-langkah keamanan, dan mengoordinasikan kebijakan lintas kementerian. Memastikan koordinasi yang komprehensif dalam implementasi kebijakan keamanan

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	other measures taken pursuant to the standards. *(iii) Evaluating the countermeasures against critical Cybersecurity-related incidents involving national administrative organs (including fact-finding activities to determine the cause or causes of the incident).* *(iv) beyond the functions listed in the preceding three items, with respect to major Cybersecurity policies: engaging in research and deliberation on program proposals; establishing cross-governmental plans, budget plans and guidelines of relevant administrative organs, the basic principles of program implementation as well as promoting the implementation of policy evaluation 8and other relevant policies; and carrying out overall coordination.* *(2) In preparing the draft of the Cybersecurity Strategy, the Headquarters must be required to hear the opinions of the Strategic Headquarters for the Promotion of an*	siber di berbagai sektor.

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	Advanced Information Telecommunications Network Society, and the National Security Council in advance. *(3) The Headquarters are to work in close coordination with the Strategic Headquarters for the Promotion of an Advanced Information elecommunications Network Society with regard to critical issues concerning Cybersecurity.* *(4) The Headquarters are to work in close coordination with the National* *Security Council with regard to critical issues concerning Cybersecurity in the context of national security."*	
Article 30	*"(1) As set by the Headquarters, the heads of the relevant administrative organs must have a duty to furnish the Headquarters timely with materials or information regarding Cybersecurity that are beneficial in fulfilling its functions.* *(2) Beyond the provision under the preceding paragraph, when requested*	Mengatur Kewajiban organ administratif terkait untuk menyediakan data atau informasi yang diperlukan oleh Headquarters untuk mendukung

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	by the Chief, the heads of the relevant administrative organs have a duty to cooperate with the Headquarters for the fulfillment of its functions, by providing materials or information regarding Cybersecurity, explanation and other necessary cooperation."	pelaksanaan fungsinya. Memastikan tersedianya data yang cukup untuk mendukung pengambilan keputusan dan pelaksanaan kebijakan keamanan siber.
Article 31	*"(1) The Headquarters may, where necessary for the fulfillment of its functions, request the submission of materials, the presentation of opinion, explanation and any other necessary cooperation from: the heads of local governments and Incorporated Administrative Agencies; the deans of national university corporations (referring to national university corporations prescribed under Article 2, paragraph (1) of the National University Corporation Act (Act No.112 of 2003)); the heads of inter-university research institute corporations (referring to inter-university research*	Wewenang Headquarters untuk meminta informasi, opini, atau kerja sama dari pihak-pihak terkait seperti pemerintah daerah dan entitas lain yang relevan guna meningkatkan efektivitas koordinasi dan kerja sama lintas sektoral dan mendukung kebijakan keamanan siber.

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
	institute corporations prescribed under Article 2, paragraph (3) of the Act); the President of the Japan Legal Support Center (referring to the Japan Legal Support Center prescribed under Article 13 of the Comprehensive Legal Support Act (Act No. 74 of 2004)); the representatives of Special Corporations and authorized corporations (referring to juridical persons incorporated by a special act and where the approval of a governmental entity is required for their incorporation and associated matters) designated by the Headquarters; and the representative of the relevant entity facilitating Cybersecurity-related communication and coordination with domestic and foreign parties concerned. *(2) In addition, the Headquarters may, where particularly necessary for the fulfillment of its functions, request necessary cooperation from a party other than the parties prescribed in the preceding paragraph."*	

Letak Norma/ Ketentuan	Materi Muatan	Maksud dan Tujuan
Article 32	*"(1) Local governments may request the provision of information and other cooperation from the Headquarters where necessary for the establishment and implementation of the policies prescribed under Article 5.* *(2) When cooperation is requested pursuant to the preceding paragraph, the Headquarters are to make an effort to meet the request."*	Ketentuan mengenai kerja sama antara pemerintah daerah dan Headquarters serta kewajiban Headquarters untuk memenuhi permintaan informasi atau dukungan yang diperlukan agar kebijakan pemerintah daerah selaras dengan strategi nasional dan kebutuhan di tingkat daerah.

Sumber: diolah Penulis (2026).

BAC mencerminkan strategi Jepang dalam menghadapi tantangan keamanan siber yang semakin kompleks. Regulasi ini memperkuat struktur kelembagaan melalui pembentukan *Cybersecurity Strategic Headquarters* sebagai pusat koordinasi nasional. BAC mengatur rincian wewenang serta tanggung jawab para pihak guna membangun kolaborasi lintas sektoral antara pemerintah pusat, daerah, dan operator infrastruktur informasi kritis. Melalui kerangka ini, Jepang tidak hanya berupaya melindungi infrastruktur nasional tetapi juga meningkatkan kesiagaan terhadap ancaman siber global.

Melalui produk hukum APPI, TBA, dan BAC, terlihat Jepang telah membangun regulasi yang komprehensif untuk melindungi data pribadi, melindungi keamanan infrastruktur digital, dan menciptakan ekosistem digital yang transparan dan terpercaya. Regulasi ini membagi tanggung jawab secara jelas antara sektor publik dan privat, serta mengedepankan kolaborasi lintas sektoral untuk menjawab tantangan global di era teknologi modern. Dengan harmonisasi regulasi yang fleksibel namun ketat, Jepang mampu menjawab kebutuhan masyarakat modern akan perlindungan data pribadi dan keamanan digital, sekaligus menjaga posisinya sebagai pemimpin global dalam tata kelola data dan keamanan siber. Hal ini menjadikan Jepang sebagai contoh bagaimana kebijakan digital dapat dirancang untuk melindungi hak individu sekaligus mendukung kemajuan teknologi.

E. Perkembangan Praktik Penyelenggara Sistem Elektronik Di Indonesia

Digitalisasi yang kian masif di berbagai sektor telah mendorong peningkatan jumlah dan variasi PSE di Indonesia. Komdigi mencatat, hingga Oktober 2024, terdapat 357 PSE lingkup publik yang telah terdaftar.[93] Sementara itu, pada lingkup privat, per Juli 2024 terdapat 11.403 PSE yang mengoperasikan 17.816 sistem elektronik.[94] Pendaftaran ini didominasi oleh tiga sektor utama: perdagangan (*marketplace*), keuangan (perbankan, *fintech*, hingga bursa kripto), serta telekomunikasi dan TI, yang meliputi media sosial, penyedia *platform,* hingga penyediaan *server*.[95] Adapun berdasarkan asalnya, sebaran

[93] Direktorat Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Digital, "Jumlah Instansi Publik yang Telah Mendaftar Penyelenggara Sistem Elektronik (PSE)", *Kementerian Komunikasi dan Digital*, https://data.komdigi.go.id/opendata/dataset/jumlah-instansi-publik-yang-telah-mendaftar-penyelenggara-sistem-elektronik-pse (diakses 10 Februari 2026).

[94] Data Sub Layanan Penyelenggara Sistem Elektronik Privat, Direktorat Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Digital RI, 5 Februari 2026

[95] Data Daftar Sistem Elektronik pada non Badan Pemerintahan, Direktorat Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Digital RI, 5 Februari 2026.

sistem elektronik privat tersebut terdiri atas 16.668 sistem elektronik domestik dan 1.148 sistem elektronik asing.[96]

Meningkatnya angka jumlah PSE khususnya di ranah privat berupa perdagangan digital turut memberikan kontribusi yang cukup signifikan terhadap perekonomian nasional. Hal tersebut tercermin dari angka penerimaan pajak dari sektor usaha ekonomi digital sebesar Rp29,97 triliun per 31 Oktober 2024.[97] Adapun rincian penerimaan tersebut berasal dari pemungutan Pajak Pertambahan Nilai (PPN) Perdagangan Melalui Sistem Elektronik (PMSE) sebesar Rp23,77 triliun, pajak kripto sebesar Rp942,88 miliar, pajak *fintech* berupa *peer-to-peer lending* sebesar Rp2,71 triliun, dan pajak yang dipungut oleh pihak lain atas transaksi pengadaan barang dan/atau jasa melalui Sistem Informasi Pengadaan Pemerintah atau Pajak SIPP sebesar Rp2,55 triliun.[98]

Besarnya ekosistem digital Indonesia, yang tercermin dari jumlah PSE serta kontribusinya terhadap ekonomi nasional belum diikuti oleh tata kelola yang baik. Berbagai persoalan dalam penyelenggaraan sistem elektronik masih kerap ditemukan, terutama yang bersumber dari kesenjangan antara regulasi (*regulatory gap*) dan perkembangan sektor tersebut.[99]

---

[96] Lihat Direktorat Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Digital, "Daftar PSE Domestik", *Kementerian Komunikasi dan Digital*, https://pse.kominfo.go.id/home/pse-domestik (diakses 10 Februari 2026); "Daftar PSE Asing", *Kementerian Komunikasi dan Digital*, https://pse.kominfo.go.id/home/pse-asing (diakses 10 Februari 2026).

[97] Direktur Penyuluhan, Pelayanan, dan Hubungan Masyarakat Direktorat Jenderal Pajak Kementerian Keuangan RI, sebagaimana dikutip dalam I. Silfia, "Pemerintah himpun pajak Rp29,97 triliun dari sektor ekonomi digital", *Antara,* https://www.antaranews.com/berita/4463121/pemerintah-himpun-pajak-rp2997-triliun-dari-sektor-ekonomi-digital (diakses 10 Februari 2026).

[98] *Ibid.*

[99] *Regulatory gap* atau kesenjangan pengaturan adalah fenomena hukum berupa kekosongan hukum yang disebabkan oleh ketiadaan hukum, ketidakmampuan peraturan perundang-undangan dalam mengatur suatu peristiwa/perbuatan hukum, serta ketidakmampuan sumber daya manusia dalam menegakkan aturan hukum. Konsep ini lazim terjadi pada negara-negara dengan sistem *civil law* yang bersandar pada peraturan perundang-undangan sebagai produk legislatif yang tidak memiliki kemampuan dalam mengatur suatu peristiwa, lihat dalam A. Kostruba, M. Haliantych, *et. al,* "Legal Gaps: Concept, Content, Problems of the Role of Legal Doctrine in Overcoming them", *Statute Law Review,* Vol. 44 (Januari 2023), 4-6.

Kesenjangan tersebut tercermin dalam terbatasnya tata kelola PSE, khususnya pada sistem kategorisasi yang ada. Saat ini, penggolongan PSE terbatas pada sektor perdagangan, keuangan, telekomunikasi/IT, hiburan/*entertainment,* serta "lainnya" untuk mengakomodasi secara sapu jagat PSE di luar kategori-kategori yang telah ada sebelumnya.

Penggolongan PSE dalam regulasi saat ini tergolong sempit sehingga gagal mengakomodasi layanan yang bersifat multi-kategori. Fenomena *social-commerce*, misalnya, mengintegrasikan media sosial dengan pasar daring (*marketplace*) dalam satu platform. Model bisnis hibrida seperti ini mengaburkan batas antar-sektor, sehingga sulit dipayungi oleh kategorisasi kaku yang ada saat ini.[100] Bentuk dari *social-commerce* yang ramai digunakan oleh masyarakat Indonesia adalah TikTokshop yang menggabungkan layanan media sosial TikTok dengan toko daring Tokopedia untuk jual beli;[101] Instagram yang awalnya hanya layanan media sosial untuk berbagi foto kini juga telah memiliki fitur *IG Shopping;*[102] dan Facebook yang tidak hanya memiliki fitur *marketplace* untuk jual-beli barang baru dan/atau bekas, tetapi juga memiliki fitur terintegrasi bagi *brand* untuk mengunggah produk, memajang katalog, hingga mempromosikan produk terkait melalui *Facebook Ads.*[103]

Selain belum tuntas mengatur *social-commerce*, tata kelola saat ini juga belum menjangkau berbagai model PSE baru yang kini marak digunakan. Salah satunya adalah kecerdasan artifisial (*artificial intelligence*/AI) atau *chatbot* seperti *Midjourney* dan *ChatGPT*, yang harusnya dikelompokkan dalam satu

---

100 H.K.S. Lam, A.C.L. Yeung, *et. al.*, "Should Firms Invest in Social Commerce? An Integrative Perspective", *Information and Management,* Vol. 56, No. 8 (Desember 2019), 4-5.

101 R. Anggraeni, "Akuisisi Tokopedia, TikTok Shop Jadi Raksasa e-Commerce Asia Tenggara", *Bisnis.com*, https://ekonomi.bisnis.com/read/20240716/12/1782611/akuisisi-tokopedia-tiktok-shop-jadi-raksasa-e-commerce-asia-tenggara (diakses 10 Februari 2026).

102 C. Newton, "Instagram is building a standalone app for shopping", *The Verge,* https://www.theverge.com/2018/9/4/17819766/instagram-shopping-app-e-commerce (diakses 10 Februari 2026).

103 N. Zuraya, "Facebook Luncurkan Fitur Belanja Shops di Indonesia", *Republika,* https://ekonomi.republika.co.id/berita/qfyu7y383/facebook-luncurkan-fitur-belanja-shops-di-indonesia (diakses 10 Februari 2026).

kategori sendiri. Tidak hanya itu, sistem AI sendiri juga telah tertanam dalam PSE sosial media, *X/Twitter* misalnya memiliki sistem *AI Grok*,[104] media sosial Meta (seperti Facebook, Instagram, dan Whatsapp) juga memiliki sistem AI Meta.[105]

Keberadaan model bisnis gabungan ini memerlukan sistem kategorisasi yang lebih luwes namun tetap memiliki standar yang jelas. Dengan regulasi yang adaptif, muncul kepastian hukum yang mampu mengikuti cepatnya perkembangan teknologi. Harapannya, tata kelola yang tangkas ini dapat memaksimalkan manfaat ekonomi digital bagi masyarakat dan negara.

Permasalahan lain dalam regulasi PSE saat ini, yaitu PP 71/2019 dan PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021, terletak pada pendekatan yang lebih mengutamakan fungsi pengawasan daripada fasilitasi, serta masih terbatasnya pengaturan perlindungan data pribadi. Terkait persoalan pertama, PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021 dinilai masyarakat sipil memuat sejumlah ketentuan yang dapat membatasi kebebasan sipil. Ketentuan tersebut meliputi, *pertama,* Pasal 9 ayat (4), yang mengatur larangan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang. Ketentuan ini dinilai dapat ditafsirkan secara bebas dan rentan digunakan untuk melakukan kriminalisasi terhadap orang atau kelompok yang mengkritik pemerintah.[106] *Kedua,* Pasal 14 ayat (3) yang mengatur penurunan konten (*takedown*). Frasa "meresahkan masyarakat" dan "mengganggu ketertiban umum" sebagai acuan untuk melakukan *takedown* dinilai tidak memiliki acuan dan klasifikasi yang jelas.[107]

---

104 B. Clinten, W.K. Pertiwi, "Pengguna X Twitter di Indonesia Sudah Bisa Coba Grok, *Chatbot AI* yang Lebih Humoris", *Kompas,* https://tekno.kompas.com/read/2024/05/10/11300077/pengguna-x-twitter-di-indonesia-sudah-bisa-coba-grok-chatbot-ai-yang-lebih (diakses 10 Februari 2026).

105 R. W. Asih, "Tak Hanya WhatsApp, Meta AI Juga Bisa Digunakan di Instagram", *Bisnis,* https://teknologi.bisnis.com/read/20241214/84/1824254/tak-hanya-whatsapp-meta-ai-juga-bisa-digunakan-di-instagram (diakses 10 Februari 2026).

106 A. Briantika, Pemblokiran PSE Dinilai Wujud Kegagalan Kominfo Urus Digitalisasi", *Tirto,* https://tirto.id/pemblokiran-pse-dinilai-wujud-kegagalan-kominfo-urus-digitalisasi-guFN (diakses 12 Februari 2026).

107 I.R.T.B. Satria, "Hidup Sungguh Amat Sederhana, tapi Dibuat Ribet Kominfo dan PSE", *Mojok,* https://mojok.co/esai/hidup-sungguh-amat-sederhana-tapi-dibuat-ribet-kominfo-dan-pse/ (diakses 12 Februari 2026).

Ketiga, ketentuan Pasal 36 yang mengizinkan aparat penegak hukum meminta konten komunikasi dan data pribadi pengguna ke PSE. Hal ini berpotensi menghilangkan jaminan keamanan data pribadi pengguna dan rawan penyalahgunaan.[108]

Persoalan lain dalam PP 71/2019 adalah terkait dengan pelindungan data pribadi. Sebagaimana telah disinggung sebelumnya, pelindungan data pribadi sebetulnya telah diatur dalam sejumlah pasal aturan tersebut, misalnya pasal terkait kewajiban PSE melaksanakan prinsip pelindungan data pribadi (Pasal 14), kewajiban menyampaikan informasi jaminan pelindungan data kepada pengguna (Pasal 29), hingga kewajiban menyediakan personel penanggung jawab pelindungan data pribadi (Pasal 32). Ketentuan tersebut kemudian diturunkan dalam PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021, di mana Pasal 3 menuntut agar permohonan pendaftaran PSE memuat informasi mengenai komitmen pelindungan data pribadi.

Meski demikian, publik menilai PP 71/2019 dan PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021 masih belum komprehensif dan bersifat sementara.[109] Setelah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU 27/2022) disahkan, sudah seharusnya sejumlah ketentuan dalam PP 71/2019 diselaraskan dengan undang-undang tersebut.

Di sisi lain, implementasi UU 27/2022 sendiri masih lemah. Hal ini disebabkan belum adanya aturan turunan, baik berupa Peraturan Pemerintah untuk melaksanakan ketentuan umum dalam undang-undang tersebut, maupun Peraturan Presiden tentang pembentukan Badan Pelindungan Data Pribadi.

Peraturan Pemerintah pelaksana UU 27/2022 merupakan instrumen krusial yang menjabarkan mekanisme implementasi berbagai mandat undang-undang tersebut, seperti prosedur pengajuan keberatan atas pemrosesan data

---

108 *Ibid.*

109 CNN Indonesia, "Pengamat Sebut PP PSTE Hanya Regulasi Sementara" *CNN Indonesia,* https://www.cnnindonesia.com/teknologi/20191023071553-185-442020/pengamat-sebut-pp-pste-hanya-regulasi-sementara (diakses 12 Februari 2026).

otomatis, tata cara pengenaan ganti rugi, hingga standar pelaksanaan pemrosesan data pribadi secara menyeluruh. Di sisi lain, efektivitas UU 27/2022 sangat bergantung pada terbentuknya lembaga otoritas pelindungan data pribadi yang mandat pembentukannya didelegasikan melalui Peraturan Presiden. Hingga saat ini, belum hadirnya kedua peraturan pelaksana tersebut menjadi catatan kritis bagi praktik PSE di Indonesia. Hal ini berdampak langsung pada operasionalisasi PSE, terutama dalam menjamin aspek keandalan dan keamanan sistem dalam melindungi data pribadi pengguna.

BAB III

EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN TERKAIT PENYELENGGARAAN SISTEM ELEKTRONIK

BAB III
EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN TERKAIT PENYELENGGARAAN SISTEM ELEKTRONIK

A. Peraturan Perundang-Undangan Vertikal di atas PP 71/2019

1. Undang-Undang Nomor 40 Tahun 1999 tentang Pers

Undang-Undang Nomor 40 Tahun 1999 tentang Pers (UU 40/1999) menegaskan keberadaan kemerdekaan pers sebagai salah satu wujud kedaulatan rakyat. Undang-undang tersebut juga mengakui bahwa kemerdekaan menyatakan pikiran dan pendapat, serta hak memperoleh informasi, merupakan hak asasi manusia yang sangat hakiki. Kemerdekaan pers dilandaskan pada prinsip-prinsip demokrasi, keadilan, dan supremasi hukum.

Prinsip-prinsip tersebut merupakan landasan pers terutama di era digital dalam melakukan kegiatannya untuk menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik. Keberadaan UU 40/1999 merupakan bagian penting dalam menjaga kedaulatan rakyat untuk mewujudkan demokrasi dan menjadikan Indonesia sebagai negara hukum khususnya terhadap poin penting penghormatan terhadap hak asasi. Catatan dan penjabaran lebih lanjut mengenai keterkaitan norma dalam UU 40/1999 dijabarkan sebagai berikut:

Tabel 3. 1. Pemetaan Ketentuan dalam UU 40/1999 yang berkaitan dengan PSE

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1.	Pasal 2 Kemerdekaan pers adalah salah satu wujud kedaulatan rakyat yang berasaskan prinsip-prinsip demokrasi, keadilan, dan supremasi hukum	Keberadaan pers dalam melaksanakan kegiatannya dilaksanakan dengan tetap mengacu pada prinsip pada hak asasi manusia.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Pasal 3 (1) Pers nasional mempunyai fungsi sebagai media informasi, pendidikan, hiburan, dan kontrol sosial (2) Di samping fungsi-fungsi tersebut ayat (1), pers nasional dapat berfungsi sebagai lembaga ekonomi	Lebih lanjut, pers nasional mempunyai hak untuk mencari, memperoleh, dan menyebarluaskan gagasan dan informasi terutama di era digital yang berkaitan dengan sistem elektronik maupun informasi elektronik di dalamnya.
	Pasal 4 (1) Kemerdekaan pers dijamin sebagai hak asasi warga negara (2) Terhadap pers nasional tidak dikenakan penyensoran, pembredelan atau pelarangan penyiaran. (3) Untuk menjamin kemerdekaan pers, pers nasional mempunyai hak mencari, memperoleh, dan menyebarluaskan gagasan dan informasi	
2.	Pasal 6 Pers nasional melaksanakan peranan sebagai berikut: a. memenuhi hak masyarakat untuk mengetahui;	Salah satu peran pers nasional adalah mengembangkan pendapat umum berdasarkan informasi di mana dalam era digital, pengembangan informasi

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	b. menegakkan nilai-nilai dasar demokrasi, mendorong terwujudnya supremasi hukum, dan Hak Asasi Manusia, serta menghormati kebhinekaan; c. mengembangkan pendapat umum berdasarkan informasi yang tepat, akurat, dan benar; d. melakukan pengawasan, kritik, koreksi, dan saran terhadap hal-hal yang berkaitan dengan kepentingan umum; e. memperjuangkan keadilan dan kebenaran.	dilaksanakan melalui berbagai media termasuk media elektronik.
3.	Pasal 17 (1) Masyarakat dapat melakukan kegiatan untuk mengembangkan kemerdekaan pers dan menjamin hak memperoleh informasi yang diperlukan.	Jaminan akan hak memperoleh informasi yang diperlukan merupakan bentuk peran serta masyarakat yang dijamin dalam UU 40/1999.

2. Undang-Undang Nomor 32 Tahun 2022 tentang Penyiaran

Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran (UU 32/2002) menegaskan perlunya membentuk sistem penyiaran nasional yang menjamin terciptanya tatanan informasi nasional yang adil, merata, dan seimbang. Tatanan tersebut dideskripsikan dalam UU 32/2002 sebagai sebuah kondisi informasi yang tertib, teratur, dan harmonis terutama mengenai arus informasi

atau pesan dalam penyiaran antara pusat dan daerah, antarwilayah di Indonesia, serta antara Indonesia dan dunia internasional. Meskipun UU 32/2002 masih menyisakan permasalahan seperti aspek pengawasan oleh Komisi Penyiaran Indonesia, tidak terlaksananya sistem stasiun jaringan yang berdampak terhadap buruknya demokratisasi penyiaran, dan permasalahan lainnya, keberadaannya tetap penting. UU 32/2022 menegaskan bahwa kemerdekaan menyampaikan pendapat dan memperoleh informasi melalui penyiaran merupakan bentuk hak asasi. Catatan dan penjabaran lebih lanjut mengenai keterkaitan norma dalam UU 32/2002 dijabarkan sebagai berikut:

Tabel 3. 2. Pemetaan Ketentuan dalam UU 32/2002 yang berkaitan dengan PSE

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1.	Pasal 4 (1) Penyiaran sebagai kegiatan komunikasi massa mempunyai fungsi sebagai media informasi, pendidikan, hiburan yang sehat, kontrol dan perekat sosial. (2) Dalam menjalankan fungsi sebagaimana dimaksud dalam ayat (1), penyiaran juga mempunyai fungsi ekonomi dan kebudayaan.	Kedua pasal tersebut menjelaskan fungsi penyiaran untuk memberikan informasi serta disaat bersamaan memiliki fungsi lainnya seperti pendidikan dan perekat sosial. Penyiaran diarahkan untuk memberikan informasi yang benar, seimbang, dan bertanggung jawab.
	Pasal 5 Penyiaran diarahkan untuk: a. menjunjung tinggi pelaksanaan Pancasila [...] b. [...]	Perkembangan teknologi telah melahirkan masyarakat informasi yang memiliki hak untuk mendapatkan informasi sehingga penyiaran sebagai penyalur

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	i. memberikan informasi yang benar, seimbang, dan bertanggung jawab;	informasi memiliki peran strategis terutama dalam mengembangkan alam demokrasi.
2.	Pasal 36 (1) Isi siaran wajib mengandung informasi, pendidikan, hiburan, dan manfaat untuk pembentukan intelektualitas, watak, moral, kemajuan, kekuatan bangsa, menjaga persatuan dan kesatuan, serta mengamalkan nilai-nilai agama dan budaya Indonesia. (2) Isi siaran dari jasa [...] (3) Isi siaran wajib memberikan perlindungan dan pemberdayaan kepada khalayak khusus, yaitu anak-anak dan remaja, dengan menyiarkan mata acara pada waktu yang tepat, dan lembaga penyiaran wajib mencantumkan dan/atau menyebutkan klasifikasi khalayak sesuai dengan isi siaran.	Pasal ini menegaskan substansi dalam isi siaran yang wajib menjaga nasionalisme serta perlindungan kepada kelompok tertentu yaitu anak dan remaja. Kaitan pasal ini dengan ketentuan penyelenggaraan sistem dan transaksi elektronik yakni substansi dalam penyelenggaraan penyiaran termasuk di era digital wajib menyesuaikan dengan substansi yang terdapat dalam UU 32/2002.

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

UU 11/2008 juncto UU 1/2024 menetapkan kerangka dasar pengaturan terhadap penyelenggaraan sistem elektronik di Indonesia. UU 11/2008 jo. UU 1/2024 juga mengatur beberapa hal fundamental dalam PSE secara umum yang sejalan dan menjadi landasan bagi ketentuan pengaturan PSE lingkup privat. Landasan tersebut meliputi pendefinisian, prinsip-prinsip, kewajiban, dan tanggung jawab dalam penyelenggaraan sistem elektronik bagi setiap pihak yang terlibat. Catatan dan penjabaran lebih lanjut norma dalam UU 11/2008 *jo.* UU 1/2024 yang berkaitan dengan PSE adalah sebagai berikut:

Tabel 3. 3. Pemetaan Ketentuan dalam UU 11/2008 jo. UU 1/2024 yang berkaitan dengan PSE.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 Angka 5 Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.	Ketentuan pendefinisian PSE dalam UU ITE telah mencakup penjabaran yang cukup komprehensif dan menjadi landasan dalam penyelenggaraan sistem elektronik secara menyeluruh baik dalam lingkup privat dan publik.
	Pasal 1 Angka 6 Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang,	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Badan Usaha, dan/atau masyarakat. Pasal 1 Angka 6A Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/ atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	
2	Pasal 3 Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi.	PSE berkaitan erat dengan pemanfaatan teknologi informasi. Oleh karena itu, setiap kegiatan penyelenggaraan sistem elektronik perlu dilandasi berdasarkan asas-asas yang diatur dalam UU ITE.
3	Pasal 15 (1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. (2) Penyelenggara Sistem Elektronik	Ketentuan Pasal *a quo* menghendaki setiap PSE untuk memberikan jaminan keamanan, keandalan, dan tanggung jawab atas Sistem Elektronik yang diselenggarakan oleh pihaknya.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	bertanggung jawab terhadap penyelenggaraan sistem elektroniknya (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik	Ketentuan dalam Pasal 15 juga menunjukkan adanya pertanggungjawaban yang dibebankan kepada PSE.
4	Pasal 16 (1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik [...]; b. dapat melindungi ketersediaan, [...]; c. dapat beroperasi sesuai dengan prosedur [...] d. dilengkapi dengan prosedur atau petunjuk yang diumumkan	Berdasarkan pengaturan tersebut, terdapat kewajiban yang harus dipenuhi sebagai standar minimum bagi setiap PSE dalam mengoperasikan Sistem Elektronik.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	dengan bahasa, [...]; dan e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, [...]	
5	Pasal 16A (1) Penyelenggara Sistem Elektronik wajib memberikan pelindungan bagi anak yang menggunakan atau mengakses Sistem Elektronik. (2) Pelindungan sebagaimana dimaksud pada ayat (1) meliputi pelindungan terhadap hak anak [...] mengenai penggunaan produk, layanan, dan fitur yang dikembangkan dan diselenggarakan oleh Penyelenggara Sistem Elektronik. (3) Dalam memberikan produk, layanan, dan fitur bagi anak, Penyelenggara Sistem Elektronik wajib menerapkan teknologi dan langkah teknis operasional [...]. (4) Dalam memberikan pelindungan sebagaimana dimaksud pada ayat (1), Penyelenggara Sistem Elektronik wajib menyediakan: a. informasi mengenai batasan	Ketentuan Pasal *a quo* merupakan penambahan dalam Revisi UU ITE terbaru (UU 1/2024) yang mewajibkan bagi PSE untuk memberikan pelindungan bagi anak yang menggunakan atau mengakses Sistem Elektronik, sesuai dengan ketentuan peraturan perundang-undangan di bidang pelindungan anak. Pelindungan tersebut melingkupi produk, layanan, dan fitur yang diberikan PSE, serta dibebani kewajiban informasi, verifikasi, dan mekanisme pelaporan penyalahgunaan yang berpotensi melanggar hak anak.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	minimum usia [...]; b. mekanisme verifikasi pengguna anak; dan c. mekanisme pelaporan penyalahgunaan produk, layanan, dan fitur yang melanggar atau berpotensi melanggar hak anak.	
6	Pasal 17 (1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat. (2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung Tambahan ayat 2(a) Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak menggunakan Tanda Tangan Elektronik yang diamankan dengan Sertifikat Elektronik.	Ketentuan ini menyebutkan bahwa dalam melakukan transaksi elektronik, terdapat kewajiban untuk memiliki itikad baik, dalam hal apabila melakukan interaksi atau pertukaran informasi maupun dokumen.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
7	Pasal 18 (1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak. (2) Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya. (3) Jika para pihak tidak melakukan pilihan [...], hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional (4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya [...]. (5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan [...] didasarkan pada asas Hukum Perdata Internasional.	Ketentuan ini menjelaskan terkait kekuatan kontrak elektronik yang sama-sama mengikat kepada para pihak seperti pada kontrak konvensional. Selain itu, ketentuan ini juga menjelaskan terkait ketentuan perdata mengenai kontrak elektronik yang sama seperti pada kontrak pada umumnya. Begitu juga berkaitan dengan kontrak elektronik Internasional yang diatur dengan hukum Indonesia. Relevansi ketentuan ini dengan PSE yakni bahwa ketentuan kontrak elektronik juga sejalan dengan penyelenggaraan sistem elektronik yang tentu bersinggungan langsung dengan penyelenggaraan kontrak dan wajib tunduk terhadap ketentuan ini.
8	Pasal 21 (1) Pengirim atau Penerima dapat melakukan Transaksi Elektronik	Ketentuan dalam Pasal *a quo* pada dasarnya memiliki keterkaitan antara

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik (2) Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut: a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi; b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau c. jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik. (3) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya	pelaksanaan transaksi elektronik serta pembebanan pertanggungjawaban dalam penyelenggaraan sistem elektronik. Hal tersebut penting untuk melihat akibat hukum yang diberikan menjadi tanggung jawab siapa. Penyelenggaraan Sistem Elektronik yang berkaitan dengan transaksi elektronik tunduk terhadap ketentuan ini dengan melihat bagaimana sistem hukum dalam ketentuan ini bekerja, baik pertanggungjawaban apabila transaksi elektronik dilakukan antara pelaku usaha dengan konsumen, maupun antara pelaku usaha dengan pelaku usaha yang lainnya.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik. (4) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.	
9	Pasal 23 (1) Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama. (2) Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain. (3) Setiap penyelenggara negara,	ketentuan ini memuat pernyataan bahwa pendaftaran domain menggunakan prinsip pendaftar pertama, artinya setiap pihak diakui kepemilikan suatu domain atas dasar siapa yang mendaftarkannya terlebih dahulu, bukan berdasarkan faktor historis. Namun, ketentuan ini juga memberikan batasan terkait penggunaan prinsip itikad baik, dan prinsip persaingan usaha yang sehat sehingga

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.	dapat melindungi PSE.
10	Pasal 26 (1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini. (3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan	Norma dalam Pasal *a quo* menghendaki adanya konsep *consent* atau persetujuan terlebih dahulu terhadap penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang. Ketentuan ini memberikan landasan bagi setiap Orang yang dilanggar hak data pribadinya untuk mengajukan gugatan atas kerugian yang ditimbulkan PSE juga terikat kewajiban atas perlindungan data pribadi tersebut serta ditambah kewajiban untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Orang yang bersangkutan berdasarkan penetapan pengadilan. (4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/ atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.	tidak relevan di bawah kendalinya dari permintaan Orang yang bersangkutan. Adapun semenjak berlakunya UU PDP, ketentuan mengenai data pribadi mengikuti ketentuan yang terdapat dalam UU 27/2022.

Sumber: diolah Penulis (2026).

4. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU 27/2022) menjadi dasar hukum dalam pengelolaan data pribadi yang diselenggarakan oleh empat subjek hukum, yaitu perseorangan, korporasi, badan publik, dan organisasi internasional. Dalam menyelenggarakan sistem dan transaksi elektronik, PSE sering kali bersinggungan dengan pemrosesan data pribadi, baik milik klien, pengguna, maupun internal organisasi. Hal ini menjadi salah satu tantangan dalam implementasi pelindungan data pribadi.

Catatan dan penjabaran lebih lanjut mengenai ketentuan dalam UU 27/2022 yang berkaitan dengan PSE adalah sebagai berikut:

Tabel 3. 4. Pemetaan Ketentuan dalam UU 27/2022 yang berkaitan dengan PSE.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 1 Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik.	PSE dalam penyelenggaraan kegiatannya berkaitan erat dengan data pribadi. Oleh karena itu, penting untuk melihat beberapa pendefinisian berkaitan dengan data pribadi maupun pelindungan data pribadi dalam ketentuan ini sebagai wujud harmonisasi terhadap peraturan perundang-undangan yang lain. Lebih lanjut, PSE dapat melakukan pengendalian maupun pemrosesan data pribadi sehingga penting untuk melakukan kontekstualisasi terhadap pendefinisian dalam Pasal serta angka *a quo* untuk PSE sebagai pengendali maupun prosesor data pribadi
	Pasal 1 angka 2 Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.	
	Pasal 1 angka 4 Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak. sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Pasal 1 angka 5 Prosesor Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.	apabila memenuhi ketentuan ini.
2	Pasal 5 Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan identitas, […]	PSE berkaitan dengan penggunaan data pribadi wajib patuh terhadap ketentuan pada pasal-pasal tersebut yang merupakan penjabaran dari hak-hak subjek data pribadi
3	Pasal 6 Subjek Data Pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data […]	
4	Pasal 8 Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/ atau memusnahkan Data […]	
5	Pasal 9 Subjek Data Pribadi berhak menarik kembali persetujuan […].	
6	Pasal 10	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Subjek Data Pribadi berhak untuk mengajukan keberatan […]	
7	Pasal 13 (1) Subjek Data Pribadi berhak mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya […] (2) Subjek Data Pribadi berhak menggunakan dan mengirimkan Data Pribadi tentang dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi […]	
8	Pasal 16 (1) Pemrosesan Data Pribadi meliputi: ' a. pemerolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan, pengumuman, transfer, penyebarluasan,	Ketentuan ini menyatakan bahwa pemrosesan data pribadi harus dilakukan dengan menghormati prinsip pelindungan data pribadi seperti harus sah secara hukum, sesuai dengan tujuannya, memberikan jaminan terhadap hak subyek data sebagaimana disebut dalam ketentuan di atas ini, serta harus dilakukan secara

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	atau pengungkapan; dan/ atau f. penghapusan atau pemusnahan. (2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (I) dilakukan sesuai dengan prinsip Pelindungan Data Pribadi meliputi: a. Data Pribadi dilakukan secara terbatas dan spesifik, [...]; b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya; c. pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi; d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, [...]; e. dst	bertanggung jawab dan dapat dibuktikan dengan jelas. Dalam konteks PSE, setiap PSE wajib patuh terhadap prinsip-prinsip pelindungan data pribadi yang termuat dalam ketentuan ini. Lebih lanjut, dalam melakukan pemrosesan data pribadi, setiap PSE juga harus mempertanggungjawabkan tindakan yang dilakukannya disertai pemberian bukti dengan jelas.
9	Pasal 20 (1) Pengendali Data Pribadi wajib memiliki dasar pemrosesan	Ketentuan ini memberikan kewajiban bagi pengendali data untuk memiliki dasar pemrosesan data pribadi

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Data Pribadi. (2) Dasar perumusan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi: a. persetujuan yang sah secara eksplisit dari Subjek Data Pribadi […]; b. pemenuhan kewajiban perjanjian dalam […]; c. pemenuhan kewajiban hukum […]; d. pemenuhan pelindungan kepentingan vital Subjek Data Pribadi; e. pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, […]; dan/atau f. pemenuhan kepentingan yang sah lainnya […].	yang harus berdasarkan persetujuan (*consent*) dari subjek data, pemenuhan kewajiban perjanjian, penghormatan terhadap hak subyek data. Kaitannya dengan PSE dalam hal ini adalah jika penyelenggara PSE sebagai sebuah entitas yang sekaligus bertindak sebagai pengendali data pribadi maka norma dalam ketentuan ini wajib untuk dipatuhi dan diperhatikan seperti adanya persetujuan (*consent*) dari subjek data dalam hal datanya akan dikendalikan olehnya.

Sumber: diolah Penulis (2026).

B. Peraturan Perundang-Undangan Horizontal

1. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

Pemerintah menerbitkan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP 80/2019) dengan tujuan mengembangkan niaga elektronik (*e-commerce*) berkelanjutan di tanah air. Penyusunan PP 80/2019 didasari tujuan untuk memberikan kesempatan berusaha yang sama (*equal playing field*) antara pelaku usaha lokal dan asing, dalam menjalankan kegiatan perdagangan daring di Indonesia. Penyusunan PP 80/2019 didasarkan pada ketentuan Pasal 65 Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan, yang bertujuan untuk membangun kepercayaan konsumen (*consumer trust*) dengan memastikan ekosistem niaga elektronik yang aman serta dapat mendorong peningkatan aktivitas dan pertumbuhan perdagangan—terutama yang diselenggarakan secara daring.

Catatan dan penjabaran lebih lanjut mengenai norma dalam PP 80/2019 yang berkaitan dengan PSE adalah sebagai berikut:

Tabel 3. 5. Pemetaan Ketentuan dalam PP 80/2019 yang berkaitan dengan PSE

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 Angka 2 Perdagangan Melalui Sistem Elektronik yang selanjutnya disingkat PMSE adalah Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik.	Ketentuan Pasal 1 PP 80/2019 memberikan definisi terhadap nomenklatur yang menjadi dasar untuk mengkualifikasikan beberapa subjek pengaturan sebagai PSE.
	Pasal 1 Angka 10 Pedagang (*merchant*) adalah Pelaku Usaha yang melakukan PMSE baik	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	dengan sarana yang dibuat dan dikelola sendiri secara langsung atau melalui sarana milik pihak PPMSE, atau Sistem Elektronik lainnya yang menyediakan sarana PMSE.	Dalam hal tersebut, Pasal 1 Angka 2 memberikan landasan pendefinisian sistem elektronik dalam konteks perdagangan elektronik. Berdasarkan definisi tersebut, terdapat 3 (tiga) subjek pengaturan yang dapat terkualifikasi sebagai PSE—dengan mengingat penyelenggaraan sistem elektronik yang dijalankan oleh subjek tersebut—yaitu: Pedagang, PPMSE, dan Penyelenggara Sarana Perantara. Ketiga subjek tersebut juga tunduk terhadap ketentuan dalam peraturan perundang-undangan terhadap PSE secara umum.
	Pasal 1 Angka 11 Penyelenggara Perdagangan Melalui Sistem Elektronik yang selanjutnya disingkat PPMSE adalah Pelaku Usaha penyedia sarana Komunikasi Elektronik yang digunakanuntuk transaksi Perdagangan.	
	Pasal 1 Angka 12 Penyelenggara Sarana Perantara (*intermediary seruices*) adalah Pelaku Usaha Dalam Negeri atau Pelaku Usaha Luar Negeri yang menyediakan sarana Komunikasi Elektronik selain penyelenggara telekomunikasi yang hanya berfungsi sebagai perantara dalam Komunikasi Elektronik antara pengirim dengan penerima.	
	Pasal 3 Dalam melakukan PMSE, para pihak harus memperhatikan prinsip: a. iktikad baik;	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	b. kehati-hatian; c. transparansi; d. keterpercayaan; e. akuntabilitas; f. keseimbangan; dan adil dan sehat.	
2	Pasal 5 Pelaku Usaha pada PMSE meliputi: a. Pelaku Usaha Dalam Negeri yang meliputi: 1. Pedagang dalam negeri; 2. PPMSE dalam negeri; dan 3. Penyelenggara Sarana Perantara dalam negeri; b. Pelaku Usaha Luar Negeri yang meliputi: 1. Pedagang luar negeri; 2. PPMSE luar negeri; dan c. Penyelenggara Sarana Perantara luar negeri.	Terdapat prinsip-prinsip penting dalam penyelenggaraan perdagangan melalui sistem elektronik, yang turut berkelindan sebagai prinsip khusus (*lex specialis*) bagi PSE yang menyelenggarakan niaga elektronik
3	Pasal 13 (1) Dalam setiap PMSE, Pelaku Usaha Wajib:	Pembagian subjek dalam Pasal 5 menegaskan pelaku usaha yang merupakan PSE penyelenggara niaga

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	a. Memberikan informasi yang benar, jelas, dan jujur tentang identitas subyek hukum yang didukung dengan data atau dokumen yang sah; b. Menyampaikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan terhadap Barang dan/atau Jasa yang diperdagangkan termasuk Sistem Elektronik yang digunakan sesuai karakteristik fungsi dan perannya dalam transaksi tersebut; dan c. Memenuhi ketentuan etika peraturan periklanan sesuai dengan ketentuan peraturan perundang-undangan. (2) Informasi yang benar, jelas, dan jujur sebagaimana dimaksud pada ayat (1) huruf a dan huruf b paling sedikit mengenai: a. kebenaran dan keakuratan informasi; b. kesesuaian antara informasi iklan dan fisik Barang;	elektronik tidak hanya mencakup dalam negeri, tetapi juga luar negeri. Hal tersebut membawa implikasi bahwa pengaturan lebih lanjut dalam PP *a quo* tidak hanya berpihak kepada salah satu pelaku usaha saja.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	c. kelayakan konsumsi Barang atau Jasa; d. legalitas Barang atau Jasa; dan 3. kualitas, harga, dan aksesibilitas Barang atau Jasa.	
4	Pasal 15 (1) Pelaku Usaha wajib memiliki izin usaha dalam melakukan kegiatan usaha PMSE. (2) Penyelenggara Sarana Perantara dikecualikan dari kewajiban memiliki izin usaha sebagaimana dimaksud pada ayat (1) jika: a. bukan merupakan pihak yang mendapatkan manfaat (*beneficiary*) secara langsung dari transaksi; atau b. tidak terlibat langsung dalam hubungan kontraktual para pihak yang melakukan PMSE. e. dst	Norma Pasal 13 PP 80/2019 memiliki muatan kewajiban yang harus dipenuhi oleh PSE yang masuk dalam kategori penyelenggara PMSE. Dalam hal tersebut, kewajiban melingkupi pemberian informasi yang benar, jelas, dan jujur terkait dengan identitas subyek hukum serta kondisi dan jaminan terhadap Barang dan/atau Jasa yang diperdagangkan. Tidak hanya itu, kewajiban bagi PSE yang menjalankan PMSE bahkan melingkupi etika mengenai periklanan.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
5	Pasal 21 ayat (1) PPMSE dalam negeri dan/atau PPMSE luar negeri wajib: a. mengutamakan menggunakan nama domain tingkat tinggi Indonesia (*dot id*) bagi Sistem Elektronik yang berbentuk situs internet; b. mengutamakan menggunakan alamat Protokol Internet (*IP Address*) sesuai dengan ketentuan peraturan perundang-undangan; c. menggunakan perangkat server yang ditempatkan di pusat data sesuai dengan ketentuan peraturan perundang-undangan; d. melakukan pendaftaran Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan; (3) dst	Norma dalam Pasal 15 PP 80/2019 mengatur mengenai kewajiban yang berlaku bagi pelaku usaha *cq.* PSE dalam sektor perdagangan melalui elektronik. Kewajiban tersebut yakni memiliki izin usaha yang dilakukan melalui Perizinan Berusaha Terintegrasi Secara Elektronik.
6	Pasal 22 ayat (1) e. Jika dalam PMSE terdapat konten informasi elektronik	Ketentuan dalam norma *a quo* mengatur mengenai kewajiban bagi PSE yang

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	ilegal, maka pihak PPMSE dalam negeri dan/atau PPMSE luar negeri serta Penyelenggara Sarana Perantara bertanggung jawab atas dampak atau konsekuensi hukum akibat keberadaan konten informasi elektronik ilegal tersebut.	merupakan PPMSE baik dalam negeri dan/atau luar negeri. Kewajiban tersebut berkaitan mulai dari penggunaan nama domain dan alamat protokol internet, penggunaan perangkat server, melakukan pendaftaran Sistem Elektronik, pemenuhan ketentuan persyaratan teknis, penyampaian data, hingga kepatuhan terhadap peraturan perundang-undangan sektoral yang berkaitan dengan perizinan kegiatan usaha PMSE.
7	Pasal 24 (1) PPMSE dalam negeri dan/atau PPMSE luar negeri wajib menjaga Sistem Elektronik yang aman, andal, dan bertanggung jawab dan membangun keterpercayaan terhadap sistem yang diselenggarakannya kepada publik.	Ketentuan *a quo* menghendaki adanya pembebanan tanggung jawab bagi PSE yang merupakan PMSE atas konten informasi elektronik ilegal. Tanggung jawab tersebut melingkupi dampak atau konsekuensi hukum akibat keberadaan konten informasi elektronik

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(2) PPMSE dalam negeri dan/atau PPMSE luar negeri wajib menyediakan pengamanan Sistem Elektronik yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian. Pengamanan Sistem Elektronik dapat mencakup pengamanan pada sisi sistem komputer PPMSE dalam negeri dan/atau PPMSE luar negeri maupun pada sisi saluran komunikasi yang digunakan dan diselenggarakan oleh pihak lain.	ilegal yang ada di *platform* mereka.
8	Pasal 25 ayat (1) PPMSE dalam negeri dan/atau PPMSE luar negeri wajib menyimpan: a. data dan informasi PMSE yang terkait dengan transaksi keuangan dalam jangka waktu paling singkat 10 (sepuluh) tahun terhitung sejak data dan informasi diperoleh; dan	Terdapat dua kewajiban dalam Pasal 24 yang diberikan kepada PSE berupa PMSE. Kedua kewajiban tersebut yaitu: kewajiban menjaga Sistem Elektronik sekaligus membangun keterpercayaan, menyediakan pengamanan Sistem Elektronik yang melingkupi sistem

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(3) data dan informasi PMSE yang tidak terkait dengan transaksi keuangan dalam jangka waktu paling singkat 5 (lima) tahun terhitung sejak data dan informasi diperoleh.	komputer maupun sisi saluran komunikasi.
9	b.	Materi muatan dalam norma *a quo* mengatur mengenai kewajiban bagi PSE yang merupakan PPMSE baik dalam maupun luar negeri untuk melakukan penyimpanan data dan informasi. Ketentuan tersebut terbagi menjadi 2 (dua) yaitu data dan informasi PMSE terkait transaksi keuangan dan yang tidak terkait transaksi keuangan.

Sumber: diolah Penulis (2026)

2. Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaran Sistem Elektronik Dalam Pelindungan Anak

Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak (PP 17/2025) merupakan ketentuan derivatif atas Pasal 16A dan Pasal 16b UU 1/2024. PP 17/2025 membahas secara komprehensif berkaitan dengan pelindungan terhadap anak

dan hak-hak anak di ruang digital. Lebih lanjut, PP 17/2025 mengatur tanggung jawab PSE dalam melakukan pelindungan terhadap anak yang menggunakan atau mengakses sistem elektronik yang dikelolanya. Oleh karena itu, substansi revisi PP 71/2019 perlu diselaraskan dengan norma-norma yang terkandung dalam PP 17/2025.

Catatan dan penjabaran lebih lanjut mengenai norma dalam PP 17/2025 yang berkaitan dengan PSE adalah sebagai berikut:

Tabel 3. 6. Pemetaan Ketentuan dalam PP 17/2025 yang berkaitan dengan PSE.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 1 Anak yang menggunakan atau atau mengakses produk, layanan, dan fitur yang selanjutnya disebut Anak adalah seseorang yang belum berusia 18 (delapan belas) tahun	Ketentuan mengatur tentang pendefinisian PSE yang didefinisikan sebagai setiap entitas yang menyediakan, mengelola, dan mengoperasikan sistem elektronik Lebih lanjut, terdapat ketentuan terkait pendefinisian anak dan data pribadi yang kemudian berkaitan dengan PSE.
	Pasal 1 angka 4 Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	

	Pasal 1 angka 5 Produk, Layanan, atau Fitur sss adalah setiap Produk, l,ayanan, dan/ atau Fitur yang dikembangkan dan/atau diselenggara}an oleh Penyelenggara Sistem Elektronik yang terhubung dengan internet atau memiliki kemampuan untuk terhubung dengan internet.	
2	Pasal 2 (1) Penyelenggara Sistem Elektronik wajib memberikan pelindungan bagi Anak yang menggunakan atau mengakses Sistem Elektronik. (2) Pelindungan sebagaimana dimaksud pada ayat (1) meliputi pelindungan terhadap hak Anak sebagaimana dimaksud dalam peraturan perundang-undangan mengenai Produk, Layanan, atau Fitur Daring yang dikembangkan dan/atau diselenggarakan oleh Penyelenggara Sistem Elektronik	Pasal *a quo* membahas terkait kewajiban PSE untuk melakukan pelindungan bagi anak yang mengakses sistem elektronik. Kemudian, Pasal ini juga mengatur tentang kewajiban menyediakan sejumlah hal mulai dari informasi mengenai batasan minimum, mekanisme verifikasi pengguna, dan mekanisme pelaporan penyalahgunaan produk yang melanggar atau berpotensi melanggar hak anak.

	(3) Dalam memberikan Produk, layanan, dan Fitur bagi Anak, Penyelenggara Sistem Elektronik wajib menerapkan teknologi dan langkah teknis operasional untuk memberikan pelindungan sebagaimana dimaksud pada ayat (1) dari tahap pengembangan sampai dengan tahap Penyelenggaraan Sistem Elektronik. (4) Dalam memberikan perlindungan sebagaimana dimaksud pada ayat (1), Penyelenggara Sistem Elektronik wajib menyediakan: a. informasi mengenai batasan minimum usia Anak yang dapat menggunakan produk atau layanannya; b. mekanisme verifikasi pengguna Anak; dan c. mekanisme pelaporan penyalahgunaan Produk, Layanan, dan Fitur yang	

	melanggar atau berpotensi melanggar hak Anak.	
3	Pasal 4 (1) Produk, Layanan, dan Fitur sebagaimana dimaksud dalam Pasal 2 meliputi: a. Produk, Layanan, dan Fitur yang secara khusus dirancang untuk digunakan atau diakses oleh Anak; atau b. Produk, Layanan, dan Fitur yang mungkin digunakan atau diakses oleh Anak (2) Produk, Layanan, dan Fitur yang mungkin digunakan atau diakses oleh Anak sebagaimana dimaksud pada ayat (1) huruf b didasarkan pada indikator: a. syarat, ketentuan, aturan, atau kebijakan yang dipublikasikan atau disusun dalam suatu dokumen internal PSE […] b. terdapat bukti kuat bahwa komposisi pengguna yang mengakses secara rutin	Ketentuan dalam Pasal *a quo* menjelaskan yang dimaksud dengan Produk, Layanan, dan Fitur yakni yang secara khusus dirancang untuk digunakan atau diakses oleh Anak atau yang mungkin digunakan atau mungkin saja digunakan atau diakses oleh Anak. Kemudian terdapat indikator-indikator tertentu terhadapnya. Keterkaitan hal ini dengan PSE yakni PSE yang menyelenggarakan sistem elektronik yang berkaitan dengan Produk, Layanan, dan Fitur yang secara khusus dirancang untuk digunakan atau diakses oleh Anak atau yang mungkin digunakan atau diakses oleh Anak wajib tunduk pada ketentuan tersebut.

	Produk, Layanan, dan Fitur tersebut adalah Anak; c. dst	
4	Pasal 5 (1) Produk, Layanan, dan Fitur sebagaimana dimaksud dalam Pasal 4 ayat (1) dinilai tingkat risikonya terhadap Anak (2) Tingkat risiko sebagaimana dimaksud pada ayat (1) terdiri atas: a. tingkat risiko tinggi; atau b. tingkat risiko rendah. (3) Penilaian tingkat risiko sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan aspek sebagai berikut: a. Berkontak dengan orang lain yang tidak dikenal; b. Terpapar pada konten pornografi, konten kekerasan, konten yang berbahaya bagi keselamatan nyawa, dan	Pasal *a quo* menjelaskan penilaian risiko terhadap Produk, Layanan, dan Fitur yang terbagi atas tingkat risiko tinggi atau tingkat risiko rendah. Lebih lanjut, Pasal 5 juga menjelaskan penilaian tingkat risiko yang dilakukan dengan memperhatikan beberapa aspek. Keterkaitan PSE dengan pasal ini yakni penyelenggaraan sistem elektronik yang berkaitan dengan Produk, Layanan, dan Fitur yang dirancang untuk digunakan atau diakses atau yang mungkin saja digunakan atau diakses oleh anak wajib memperhatikan tingkat risiko maupun penilaian risiko terhadapnya.

	konten lain yang tidak sesuai peruntukan Anak; c. eksploitasi Anak sebagai konsumen; d. mengancam keamanan Data Pribadi Anak; e. menimbulkan adiksi; f. gangguan kesehatan psikologis Anak; dan g. gangguan fisiologis Anak. (4) Jika Produk, Layanan, dan Fitur memiliki […] (5) dst	
5	Pasal 7 (1) Dalam memberikan pelindungan Anak sebagaimana dimaksud dalam Pasal 2 ayat (l), ayat (2), dan ayat (3), Penyelenggara Sistem Elektronik melaksanakan kewajiban yang meliputi: a. mendapatkan persetujuan dari orang tua atau wali Anak;	Pasal *a quo* menjelaskan kewajiban-kewajiban bagi PSE dalam upaya memberikan pelindungan anak antara lain mendapatkan persetujuan (*consent*), menyusun penilaian dampak pelindungan data pribadi, dll. Selain itu terdapat larangan secara tegas bagi PSE untuk menggunakan praktik terselubung atau tidak transparan, mengumpulkan

	b. menyusun Penilaian Dampak Pelindungan Data Pribadi; c. Mengonfigurasi pengaturan Produk, Layanan, dan Data Fitur yang secara khusus dirancang untuk digunakan atau diakses oleh Anak atau yang mungkin digunakan atau diakses oleh Anak dalam tingkat privasi tinggi secara baku; d. memberikan informasi yang lengkap, benar, akurat, dan tidak bagl pengguna untuk memahami Produk, Layanan, dan Fitur; e. melakukan edukasi dan pemberdayaan ekosistem digital; f. dst (2) Dalam memberikan pelindungan Anak sebagaimana dimaksud dalam Pasal 2 ayat (I), ayat (2), dan ayat (3),	informasi geolokasi yang tepat dari Anak, dan melakukan *profiling*. Pasal ini juga menjelaskan perlunya penilaian dampak pelindungan data pribadi serta penunjukan *Data Protection Officer* yang mengikuti ketentuan peraturan perundang-undangan bidang pelindungan data pribadi.

	Penyelenggara Sistem Elektronik dilarang: a. menggunakan atau menerapkan cara, teknik, atau praktik terselubung atau tidak transparan dalam pengembangan atau penyelenggaraan Produk, Layanan, dan Fitur; b. mengumpulkan informasi geolokasi yang tepat dari Anak; dan c. melakukan pemrofilan Anak (3) Penyusunan Penilaian Dampak Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) huruf b dan penunjukan pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi sebagaimana dimaksud pada ayat (l) huruf j, dilaksanakan sesuai dengan ketentuan peraturan perundang-undanga	

6	Pasal 8 Dalam melaksanakan pelindungan sebagaimana dimaksud dalam Pasal 2, PSE: a. Mempertimbangkan kepentingan terbaik bagi Anak dalam mengembangkan dan/atau menyelenggarakan Produk, Layanan, dan Fitur yang secara khusus dirancang untuk digunakan atau diakses oleh Anak, atau yang mungkin digunakan atau diakses oleh Anak; dan b. memprioritaskan pemenuhan hak Anak dan pelindungan terhadap Anak dibandingkan dengan kepentingan komersial Penyelenggara Sistem Elektronik.	Pasal ini menjelaskan adanya keharusan PSE mempertimbangkan kepentingan terbaik bagi anak dan memprioritaskan pemenuhan hak anak dan pelindungannya dibandingkan dengan kepentingan komersial PSE. Keharusan pada Pasal 8 PP *a quo* selaras dengan berbagai kewajiban yang diatur pada pasal-pasal berikutnya dalam PP 17/2025.

Sumber: Diolah Penulis (2026).

C. Peraturan Perundang-Undangan Vertikal di bawah PP 71/2019

1. Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas

Penerbitan Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas (Perpres 32/2024) didasari oleh perhatian pemerintah terhadap jurnalisme berkualitas dan keberlanjutan industri media konvensional. Pertimbangan pemerintah untuk menerbitkan Perpres *a quo* didasari pula oleh kedudukan jurnalisme berkualitas sebagai salah satu pilar dalam kehidupan negara dan masyarakat yang demokratis, serta perlu adaptif dengan perkembangan dan dukungan perusahaan *platform* digital.[110] Adaptasi terhadap perkembangan teknologi informasi menjadi pendorong dalam praktik jurnalisme berkualitas, sehingga pemerintah merasa perlu untuk mengatur ekosistem dan hubungan antara perusahaan platform digital dengan perusahaan pers dalam mendukung jurnalisme berkualitas di Indonesia.[111]

Ruang lingkup Perpres 32/2024 mencakup perusahaan platform digital, kerja sama platform digital dengan perusahaan pers, komite, serta pendanaan. Berdasarkan ruang lingkup pengaturan tersebut, maka perusahaan *platform* digital dapat dikategorikan sebagai salah satu bentuk PSE khusus yang menjadi ranah pengaturan dari Perpres *a quo.* Keterkaitan dari kedudukan perusahaan *platform* digital sebagai PSE khusus di bidang jurnalisme sebagaimana diatur dalam Perpres 32/2024, dijabarkan dalam tabel sebagai berikut:

Tabel 3.7. Pemetaan Ketentuan dalam Perpres 32/2024 yang berkaitan dengan PSE

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 1 Tanggung Jawab Perusahaan Platform Digital adalah kewajiban perusahaan platform digital	Definisi nomenklatur *a quo* menghendaki adanya tanggung jawab perusahaan platform digital sebagai upaya mendukung

[110] Humas Sekretariat Kabinet RI, "Inilah Perpres 32/2024 tentang *Publisher Rights*", Sekretariat Kabinet RI, https://setkab.go.id/inilah-perpres-32-2024-tentang-publisher-rights/ (diakses 20 Februari 2026).

[111] *Ibid.*

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	menjaga ekosistem bisnis pemberitaan yang sehat untuk mendukung jurnalisme berkualitas.	jurnalisme berkualitas. Oleh sebab itu, perusahaan platform digital yang masuk dalam kategori PSE khusus ini dibebani tanggung jawab tersebut.
	Pasal 1 angka 4 Layanan Platform Digital adalah layanan milik perusahaan platform digital yang meliputi pengumpulan, pengolahan, pendistribusian, dan penyajian Berita secara digital serta interaksi dengan Berita yang berfungsi memperantarai layanan penyajian Berita yang ditujukan terutama untuk bisnis.	Definisi nomenklatur *a quo* mengatur ruang lingkup layanan platform digital sebagai layanan milik perusahaan platform digital untuk mengumpulkan, mengolah, mendistribusi, serta menyajikan berita secara digital serta sebagai perantara layanan penyajian berita yang ditujukan untuk bisnis. Ketentuan tersebut merupakan ruang lingkup dari layanan platform digital sebagai PSE di bidang jurnalisme digital.
	Pasal 1 angka 9 Perusahaan Platform Digital adalah penyelenggara sistem elektronik lingkup privat yang menyediakan dan menjalankan Layanan Platform Digital serta memanfaatkannya	Definisi nomenklatur *a quo* menegaskan kedudukan perusahaan platform digital sebagai PSE lingkup privat yang menyediakan dan menjalankan Layanan

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	untuk tujuan komersial melalui pengumpulan dan pengolahan data.	Platform Digital beserta pemanfaatannya untuk tujuan komersial dengan pengumpulan dan pengolahan data.
2	Pasal 2 Peraturan Presiden ini bertujuan mengatur tanggung jawab Perusahaan Platform Digital untuk mendukung jurnalisme berkualitas agar Berita yang merupakan karya jurnalistik dihormati dan dihargai kepemilikannya secara adil dan transparan.	Pasal *a quo* mengatur tujuan dari keberadaan Perpres *a quo* sebagai upaya mengatur Perusahaan Platform Digital sebagai PSE lingkup privat dalam rangka mendukung jurnalisme berkualitas agar berita sebagai karya jurnalistik dapat dihormati dan dihargai kepemilikannya secara adil dan transparan.
3	Pasal 4 Perusahaan Platform Digital ditetapkan berdasarkan kehadiran Layanan Platform Digital di Indonesia.	Pasal *a quo* mengatur penetapan terhadap Perusahaan Platform Digital sebagai PSE lingkup privat didasarkan pada kehadiran Layanan Platform Digital di Indonesia.
4	Pasal 5 Perusahaan Platform Digital sebagaimana dimaksud dalam Pasal	Pasal *a quo* mengatur kewajiban bagi PSE Perusahaan Platform Digital untuk mendukung

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	4 wajib mendukung jurnalisme berkualitas dengan: a. tidak memfasilitasi penyebaran dan/atau tidak melakukan komersialisasi konten Berita yang tidak sesuai dengan Undang-Undang mengenai pers setelah menerima laporan melalui sarana pelaporan yang disediakan oleh Perusahaan Platform Digital; b. memberikan upaya terbaik untuk membantu memprioritaskan fasilitasi dan komersialisasi Berita yang diproduksi oleh Perusahaan Pers; c. memberikan perlakuan yang adil kepada semua Perusahaan Pers dalam menawarkan Layanan Platform Digital; d. melaksanakan pelatihan dan program yang ditujukan untuk mendukung jurnalisme yang berkualitas dan bertanggung jawab;	jurnalisme berkualitas dengan tata cara yang telah diatur dalam Pasal 5 huruf a sampai dengan huruf b.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	e. memberikan upaya terbaik dalam mendesain Algoritma distribusi Berita yang mendukung perwujudan jurnalisme berkualitas sesuai dengan nilai demokrasi, kebhinekaan, dan peraturan perundang-undangan; dan f. bekerja sama dengan Perusahaan Pers.	
5	Pasal 7 (1) Kerja sama Perusahaan Platform Digital dengan Perusahaan Pers dituangkan dalam perjanjian. (2) Kerja sama sebagaimana dimaksud pada ayat (1) berupa: a. lisensi berbayar; b. bagi hasil; c. berbagi data agregat pengguna Berita; dan/atau d. bentuk lain yang disepakati. (3) Bagi hasil sebagaimana dimaksud pada ayat (21 huruf b merupakan pembagian	Pasal *a quo* mengatur dan menghendaki adanya kerja sama antara PSE Perusahaan Platform Digital dengan Perusahaan Pers untuk dituangkan dalam perjanjian, yang memuat: lisensi berbayar, bagi hasil, berbagi data agregat pengguna berita, dan/atau bentuk lain yang disepakati. Bagi hasil dalam kerja sama tersebut diwujudkan dalam pembagian pendapatan atas pemanfaatan berita oleh PSE Perusahaan Platform Digital yang diproduksi Perusahaan Pers

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	pendapatan atas pemanfaatan Berita oleh Perusahaan Platform Digital yang diproduksi Perusahaan Pers berdasarkan perhitungan nilai keekonomian.	berdasarkan perhitungan nilai ekonomi.

Sumber: diolah Penulis (2026).

2. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 (PM Kominfo 5/2020 jo. PM Kominfo 10/2021) memberikan ketentuan mengenai kriteria dan persyaratan PSE Lingkup Privat. Lebih lanjut, PM Kominfo *a quo* mengatur rangkaian tindakan penyelenggara sistem elektronik mulai dari tahapan pendaftaran, tata kelola data dan informasi, hingga ketentuan terkait pemberian akses data bagi kepentingan pengawasan. Penjabaran lebih lanjut mengenai keterkaitan norma dalam PM Kominfo 5/2020 jo. PM Kominfo 10/2021 adalah sebagai berikut:

Tabel 3. 8. Pemetaan Ketentuan dalam PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021 yang berkaitan dengan PSE, khususnya PSE Lingkup Privat.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 5 Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	Penyelenggara Sistem Elektronik dalam ketentuan ini dijabarkan sebagai pihak-pihak yang menyediakan, mengelola, dan/atau mengoperasi kan sistem elektronik. Lebih lanjut, terhadap penyelenggara sistem elektronik lingkup privat merupakan penyelenggara oleh orang, badan, usaha, dan masyarakat. Pasal *a quo* memberikan berbagai pendefinisian yang relevan dan dapat sebagai bahan harmonisasi definisi dengan pendefinisian peraturan perundang-undangan lain terkait PSE.
	Pasal 1 angka 6 Penyelenggara Sistem Elektronik Lingkup Privat yang selanjutnya disebut PSE Lingkup Privat adalah penyelenggaraan Sistem Elektronik oleh orang, badan usaha, dan masyarakat.	
	Pasal 1 angka 7 PSE Lingkup Privat *User Generated Content* adalah PSE Lingkup Privat yang penyediaan, penayangan, pengunggahan, dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektroniknya dilakukan oleh Pengguna Sistem Elektronik.	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Pasal 1 angka 8 Pengguna Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik.	
	Pasal 1 angka 11 Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau non elektronik.	
	Pasal 1 angka 12 Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	Pasal 1 angka 21 Data Pribadi Spesifik adalah data dan informasi kesehatan, data biometrik, data genetika, kehidupan/orientasi seksual, pandangan politik, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.	
2	Pasal 2 (1) Setiap PSE Lingkup Privat wajib melakukan pendaftaran. (2) PSE Lingkup Privat sebagaimana dimaksud pada ayat (1) meliputi: a. Penyelenggara Sistem Elektronik yang diatur atau diawasi oleh Kementerian atau Lembaga berdasarkan ketentuan peraturan perundang-undangan; dan/atau b. Penyelenggara Sistem Elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet yang dipergunakan untuk 1. menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau	Ketentuan ini mengatur kewajiban terhadap penyelenggara sistem elektronik lingkup privat untuk melakukan pendaftaran. Lebih lanjut, Peraturan *a quo* mengatur kualifikasi penyelenggara sistem elektronik yang termasuk sebagai penyelenggara lingkup privat seperti penyelenggara yang diatur dan diawasi oleh K/L, penyelenggara sistem elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan internet, dan sebagainya.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	perdagangan barang dan/atau jasa; 2. menyediakan, mengelola, dan/atau mengoperasikan layanan transaksi keuangan; 3. pengiriman materi atau muatan digital berbayar melalui jaringan data baik dengan cara unduh melalui portal atau situs, pengiriman lewat surat elektronik, atau melalui aplikasi lain ke perangkat Pengguna Sistem Elektronik; 4. menyediakan, mengelola, dan/atau mengoperasikan layanan komunikasi meliputi namun tidak terbatas pada pesan singkat, panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial; (3) Kewajiban melakukan pendaftaran bagi PSE Lingkup Privat dilakukan sebelum Sistem Elektronik mulai	Selain itu, ketentuan ini juga mewajibkan kepada PSE lingkup privat yang berdomisili di luar Indonesia tetapi melakukan usaha di Indonesia untuk melakukan pendaftaran ke pemerintah Indonesia.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	digunakan oleh Pengguna Sistem Elektronik. (4) Pendaftaran ISP sebagai PSE Lingkup Privat dilaksanakan melalui perizinan yang diselenggarakan oleh Kementerian sesuai dengan ketentuan peraturan perundang-undangan (5) Masyarakat dapat memberikan pengaduan/informasi terhadap PSE Lingkup Privat yang tidak melakukan kewajiban pendaftaran.	
3	Pasal 4 (1) Kewajiban PSE Lingkup Privat melakukan pendaftaran sebagaimana dimaksud dalam Pasal 2 ayat (1) juga berlaku untuk PSE Lingkup Privat yang didirikan menurut hukum negara lain atau yang berdomisili tetap di negara lain tetapi: a. memberikan layanan di dalam wilayah Indonesia; b. melakukan usaha di Indonesia; dan/atau c. Sistem Elektroniknya dipergunakan dan/atau	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	ditawarkan di wilayah Indonesia. (2) Pendaftaran PSE Lingkup Privat sebagaimana dimaksud pada ayat (1) dilakukan dengan mengisi formulir pendaftaran yang memuat informasi sebagaimana dimaksud dalam Pasal 3 ayat (3) dan Pasal 3 ayat (4) serta informasi yang benar yang meliputi: a. identitas PSE Lingkup Privat; b. identitas pimpinan perusahaan dan/atau identitas penanggung jawab; c. keterangan domisili dan/atau akta pendirian perusahaan (*certificate of incorporation*); d. jumlah pelanggan (*user*) dari Indonesia; dan e. nilai transaksi yang berasal dari Indonesia. (3) Informasi sebagaimana dimaksud pada ayat (2) huruf c disampaikan dengan melampirkan dokumen pendukung yang diterjemahkan ke dalam bahasa Indonesia oleh penerjemah tersumpah.	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
4	Pasal 7 (1) Menteri mengenakan sanksi administratif kepada PSE Lingkup Privat yang: a. tidak melakukan pendaftaran sebagaimana dimaksud dalam Pasal 2 dan Pasal 4; b. telah mempunyai tanda daftar tetapi tidak melaporkan perubahan terhadap informasi pendaftaran sebagaimana dimaksud dalam Pasal 5; c. tidak memberikan informasi pendaftaran sebagaimana dimaksud dalam Pasal 3 ayat (3), Pasal 3 ayat (4), dan Pasal 4 ayat (2) dengan benar. (2) Dalam hal PSE Lingkup Privat tidak melakukan pendaftaran sebagaimana dimaksud pada ayat (1) huruf a, Menteri memberikan sanksi administratif berupa Pemutusan Akses terhadap Sistem Elektronik (access blocking). (3) Dalam hal PSE Lingkup Privat telah mempunyai tanda daftar tetapi tidak melaporkan perubahan terhadap informasi pendaftaran	Pasal *a quo* mengatur ketentuan pemberian sanksi kepada penyelenggara sistem elektronik lingkup privat yang tidak melakukan pendaftaran, telah mempunyai tanda daftar tetapi tidak melaporkan perubahan, atau tidak memberikan informasi pendaftaran. Adapun sanksi tersebut diberikan secara berjenjang mulai dari teguran tertulis, pembatasan akses sementara, hingga pemutusan akses (*access blocking*) terhadap aktivitas penyelenggaraan sistem elektronik yang dilakukannya.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sebagaimana dimaksud pada ayat (1) huruf b atau tidak memberikan informasi pendaftaran dengan benar sebagaimana dimaksud pada ayat (1) huruf c, Menteri memberikan sanksi administratif berupa: a. teguran tertulis yang disampaikan melalui surat elektronik (*electronic mail*) dan/atau media elektronik lainnya; b. penghentian sementara terhadap PSE Lingkup Privat dalam hal tidak mengindahkan teguran tertulis sebagaimana dimaksud pada ayat (3) huruf a; c. Pemutusan Akses terhadap Sistem Elektronik (*access blocking*) dan pencabutan Tanda Daftar Penyelenggara Sistem Elektronik dalam hal PSE Lingkup Privat tidak memberikan konfirmasi dalam jangka waktu 7 (tujuh) hari setelah penghentian sementara sebagaimana dimaksud pada ayat (3) huruf b. (4) Dalam hal PSE Lingkup Privat telah	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	memenuhi ketentuan pendaftaran sebagaimana dimaksud dalam Pasal 2 sampai dengan Pasal 5, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang diputus aksesnya (*access blocking*) sebagaimana dimaksud pada ayat (2). (5) Dalam hal PSE Lingkup Privat telah melakukan pembaruan informasi pendaftaran dengan benar, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang dihentikan sementara sebagaimana dimaksud pada ayat (3) huruf b. (6) Dalam hal PSE Lingkup Privat telah melakukan pendaftaran ulang dengan memberikan informasi pendaftaran dengan benar, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang diputus akses Sistem Elektroniknya dan dicabut tanda daftar Penyelenggara Sistem Elektroniknya sebagaimana dimaksud pada ayat (3) huruf c.	
5	Pasal 9 (1) PSE Lingkup Privat bertanggung	Ketentuan ini mengatur tanggung jawab penyelenggara sistem

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	jawab atas penyelenggaraan Sistem Elektronik dan pengelolaan Informasi Elektronik dan/atau Dokumen Elektronik di dalam Sistem Elektronik secara andal, aman, dan bertanggung jawab. (2) PSE Lingkup Privat wajib menyediakan petunjuk penggunaan layanan dalam bahasa Indonesia sesuai dengan ketentuan perundang-undangan. (3) PSE Lingkup Privat wajib memastikan: a. Sistem Elektroniknya tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang; dan b. Sistem Elektroniknya tidak memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang. (4) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3) dengan klasifikasi: a. melanggar ketentuan peraturan	elektronik lingkup privat terhadap PSE yang harus dilaksanakan secara andal, aman, dan bertanggung jawab. Maksudnya ialah penyelenggaraan sistem elektronik lingkup privat harus dapat membangun kepercayaan penggunanya, memuat standar keamanan yang tinggi dan dalam penyelenggaraannya harus dapat mempertanggungjawabkan segala kegiatan yang dilakukan dengan bukti yang jelas. Lebih lanjut, ketentuan ini memberikan kewajiban dalam penyelenggaraannya. PSE lingkup privat dilarang memuat informasi atau dokumen elektronik yang dilarang seperti melanggar ketentuan, meresahkan

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	perundang-undangan; b. meresahkan masyarakat dan mengganggu ketertiban umum; dan c. memberitahukan cara atau menyediakan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang. (5) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (4) huruf b ditetapkan oleh Kementerian atau Lembaga sesuai dengan ketentuan peraturan perundang-undangan. (6) PSE Lingkup Privat yang tidak melakukan kewajiban sebagaimana dimaksud pada ayat (3) diputus akses terhadap Sistem Elektroniknya (*access blocking*) sesuai dengan ketentuan dalam Peraturan Menteri ini.	masyarakat, ataupun memuat informasi yang memberitahukan cara untuk mengakses informasi elektronik dan/atau dokumen yang dilarang. Adapun terhadap penyelenggara sistem elektronik lingkup privat yang tidak mematuhi ketentuan ini akan diberikan sanksi administratif.
6	Pasal 13 (1) PSE Lingkup Privat wajib melakukan Pemutusan Akses (*take down*) terhadap Informasi Elektronik	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 9 ayat (4). (2) Kewajiban melakukan Pemutusan Akses (take down) sebagaimana dimaksud pada ayat (1) termasuk Pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dapat memfasilitasi penyebarluasan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.	
7	Pasal 20 (1) PSE Lingkup Privat yang diputus akses terhadap Sistem Elektroniknya (*access blocking*) atau Kementerian atau Lembaga dapat mengajukan permohonan Normalisasi kepada Menteri. (2) Permohonan Normalisasi oleh PSE Lingkup Privat yang diputus akses terhadap Sistem Elektroniknya (*access blocking*) sebagaimana dimaksud pada ayat (1) diajukan dengan melampirkan: a. surat permohonan tertulis; b. identitas penanggung jawab Sistem Elektronik dan nomor	Ketentuan ini mengatur terkait mekanisme normalisasi terhadap penyelenggara sistem elektronik lingkup privat yang diputus aksesnya yang dilakukan melalui pengajuan permohonan normalisasi kepada menteri. Lebih lanjut, terhadap permohonan tersebut diberikan daftar lampiran yang harus dipenuhi agar permohonan tersebut dapat diterima.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	kontak yang dapat dihubungi; c. hasil pindai kartu identitas pemilik dan/atau penanggung jawab Sistem Elektronik; d. gambar atau *screen capture* dan tautan atau *link* (URL) yang membuktikan bahwa Sistem Elektronik tidak lagi memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang; e. surat rekomendasi dari Kementerian atau Lembaga, Aparat Penegak Hukum, atau putusan pengadilan yang berkekuatan hukum tetap; dan f. bukti lainnya yang mendukung legitimasi sebagai PSE Lingkup Privat. (3) (3) Permohonan Normalisasi oleh Kementerian atau Lembaga sebagaimana dimaksud pada ayat (1) diajukan melalui surat permohonan tertulis. (4) Menteri menindaklanjuti permohonan Normalisasi yang memenuhi persyaratan sebagaimana dimaksud pada ayat	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(2) dan ayat (3) dalam waktu paling lama 2x24 (dua kali dua puluh empat) jam. (5) Menteri berwenang menolak permohonan Normalisasi terhadap Sistem Elektronik yang telah diputus aksesnya (*access blocking*) lebih dari 3 (tiga) kali.	
8	Pasal 21 (1) PSE Lingkup Privat wajib memberikan akses terhadap Sistem Elektronik dan/atau Data Elektronik kepada Kementerian atau Lembaga dalam rangka pengawasan sesuai dengan peraturan perundang-undangan. (2) PSE Lingkup Privat wajib memberikan akses terhadap Sistem Elektronik dan/atau Data Elektronik kepada Aparat Penegak Hukum dalam rangka penegakan hukum sesuai dengan peraturan perundang-undangan.	Dalam ketentuan ini, Penyelenggara sistem elektronik lingkup privat harus mematuhi ketentuan untuk memberikan akses terhadap sistem atau data elektronik yang dimilikinya kepada K/L dalam rangka pengawasan. Selain itu, penyelenggara sistem elektronik lingkup privat dapat dimintakan untuk diakses sistem atau data elektroniknya untuk kepentingan penegakan hukum pidana dimana dalam ketentuan ini

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
		diatur batas minimum tindak pidana yang dapat dimintakan akses tersebut, yaitu tindak pidana yang memiliki ancaman pidana paling singkat 2 (dua) tahun.
9	Pasal 32 (1) PSE Lingkup Privat memberikan akses terhadap Data Elektronik kepada Aparat Penegak Hukum untuk kepentingan penyidikan, penuntutan, atau persidangan tindak pidana dalam wilayah hukum Negara Kesatuan Republik Indonesia. (2) Tindak pidana yang dimaksud pada ayat (1) adalah tindak pidana yang ancaman pidananya berupa pidana penjara paling singkat 2 (dua) tahun.	
10	Pasal 43 (1) PSE Lingkup Privat wajib memiliki rekam jejak audit mengenai penggunaan akses terhadap Sistem Elektronik yang dilakukan oleh Kementerian atau Lembaga. (2) PSE Lingkup Privat dapat melakukan	Dalam hal ini, penyelenggara sistem elektronik lingkup privat diberikan kewajiban untuk memiliki rekam jejak audit mengenai penggunaan akses terhadap sistem

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	penilaian (*assessment*) mengenai dampak penggunaan akses terhadap Sistem Elektronik oleh Kementerian atau Lembaga terhadap: a. kualitas layanan yang diberikan PSE Lingkup Privat kepada Pengguna Sistem Elektroniknya; b. pelindungan Data Pribadi dari Pengguna Sistem Elektroniknya; dan/atau c. pemenuhan kewajiban PSE Lingkup Privat yang diatur dalam peraturan perundang-undangan Indonesia. (3) Penggunaan akses untuk kepentingan pengawasan dilakukan dalam jangka waktu wajar dan dapat dipertanggungjawabkan.	elektronik yang dimilikinya yang dilakukan oleh K/L serta Aparat Penegakan Hukum.
11	Pasal 44 (1) PSE Lingkup Privat wajib memiliki rekam jejak audit mengenai penggunaan akses terhadap Sistem Elektronik yang dilakukan oleh Aparat Penegak Hukum. (2) PSE Lingkup Privat dapat melakukan	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	penilaian (*assessment*) mengenai dampak penggunaan akses terhadap Sistem Elektronik oleh Aparat Penegak Hukum terhadap: a. kualitas layanan yang diberikan PSE Lingkup Privat kepada Pengguna Sistem Elektroniknya; b. pelindungan Data Pribadi dari Pengguna Sistem Elektroniknya; dan/atau c. pemenuhan kewajiban PSE Lingkup Privat yang diatur dalam peraturan perundang-undangan Indonesia. (3) Penggunaan akses untuk kepentingan penegakan hukum dilakukan dalam jangka waktu wajar dan dapat dipertanggungjawabkan.	

Sumber: diolah Penulis (2026).

3. Peraturan Menteri Perdagangan Nomor 31 Tahun 2023 tentang Perizinan Berusaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan melalui Sistem Elektronik

Kementerian Perdagangan menerbitkan Peraturan Menteri Perdagangan Nomor 31 Tahun 2023 tentang Perizinan Berusaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan Melalui Sistem Elektronik (PM Dag 31/2023) sebagai respons atas perkembangan perdagangan elektronik di

Indonesia. Perkembangan Perkembangan tersebut menuntut adanya standardisasi dalam platform PMSE, dengan memperhatikan berbagai permasalahan seperti indikasi perdagangan tidak sehat oleh pelaku usaha asing; masih lemahnya daya saing produk dalam negeri serta usaha mikro kecil dan menengah (UMKM); masih belum terwujudnya persaingan yang setara dalam ekosistem PMSE; dan munculnya model bisnis baru yang berpotensi mengganggu ekosistem PMSE di Indonesia.[112] Tujuan penyusunan dan penerbitan PM Dag 31/2023 adalah menciptakan ekosistem yang sehat, dengan memperhatikan perkembangan teknologi yang dinamis; mendukung pemberdayaan UMKM dan pelaku usaha PMSE dalam negeri; dan meningkatkan pelindungan konsumen dalam negeri.

Pengaturan dalam PM Dag 31/2023 memuat enam poin penting terkait penyelenggaraan PMSE, yaitu: (1) pendefinisian model bisnis PMSE yang baru, seperti *marketplace* atau loka pasar dan *social commerce* dalam rangka kemudahan pembinaan dan pengawasan; (2) penetapan harga minimum sebesar US$ 100 per unit untuk barang jadi asal luar negeri yang langsung dijual oleh pedagang ke Indonesia melalui platform *e-commerce* lintas negara; (3) penyediaan *positive list* atau daftar barang asal luar negeri yang diperbolehkan lintas negara secara langsung masuk Indonesia melalui platform *e-commerce;* (4) menetapkan syarat khusus bagi pedagang luar negeri pada *marketplace* dalam negeri; (5) larangan *marketplace* dan *social commerce* bertindak sebagai produsen; dan (6) larangan penguasaan data oleh PPSE dan afiliasi, guna memastikan tidak terjadi penyalahgunaan penguasaan data pengguna untuk dimanfaatkan PPMSE atau perusahaan afiliasinya.[113] Rincian keterkaitan PM Dag 31/2023 dengan PSE dapat dilihat dalam tabel pemetaan berikut:

---

[112] Kementerian Perdagangan RI, "Menteri Perdagangan Resmi Berlakukan Permendag 31/2023", *Kementerian Perdagangan RI*, https://www.kemendag.go.id/berita/pojok-media/zulhas-resmi-berlakukan-permendag-312023 (diakses 21 Februari 2026).

[113] *Ibid.*

Tabel 3. 9. Pemetaan Ketentuan dalam PM Dag 31/2023 yang berkaitan dengan PSE, khususnya PSE Lingkup Privat dan yang menyelenggarakan perdagangan melalui sistem elektronik.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 2 Perdagangan Melalui Sistem Elektronik yang selanjutnya disingkat PMSE adalah Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik.	Pasal 1 PMDag *a quo* memberikan definisi atas sejumlah nomenklatur pengaturan dalam materi muatan Peraturan Menteri *a quo.* Adapun dalam definisi tersebut, terdapat sejumlah aktor yang terkategori menjadi PSE lingkup privat di bidang perdagangan melalui sistem elektronik. Sejumlah aktor tersebut yaitu misalnya Pedagang, PSP, *Merchant,* Lokapasar, Media Sosial, Pelantar, dan *Social-Commerce.* Landasan dari kategorisasi tersebut adalah adanya penggunaan dan penyelenggaraan sistem elektronik oleh aktor tersebut dalam menjalankan kegiatan perdagangan elektronik. Selain itu, definisi dalam Pasal *a quo* menghendaki agar aktor yang terlibat dalam penyelenggaraan PMSE untuk
	Pasal 1 angka 6 Pelaku Usaha Perdagangan Melalui Sistem Elektronik yang selanjutnya disebut Pelaku Usaha adalah setiap orang perseorangan atau badan usaha yang berbentuk badan hukum atau bukan badan hukum yang dapat berupa pelaku usaha dalam negeri dan pelaku usaha yang berkedudukan di luar negeri dan melakukan kegiatan usaha di bidang PMSE.	
	Pasal 1 angka 9 Penyelenggara Perdagangan Melalui Sistem Elektronik yang selanjutnya disingkat PPMSE adalah Pelaku Usaha penyedia sarana	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	komunikasi elektronik yang digunakan untuk transaksi Perdagangan.	dibebankan kewajiban perizinan sekaligus adanya mekanisme penegakan hukum dengan pemutusan akses terhadap setiap pihak yang melanggar ketentuan PMDag *a quo* maupun peraturan perundang-undangan terkait.
	Pasal 1 angka 10 Pedagang (*Merchant*) adalah Pelaku Usaha yang melakukan PMSE dengan sarana yang dibuat dan dikelola sendiri secara langsung atau melalui sarana milik pihak PPMSE, atau Sistem Elektronik lainnya yang menyediakan sarana PMSE.	
	Pasal 1 angka 11 Penyelenggara Sarana Perantara (*Intermediary Services*) yang selanjutnya disingkat PSP adalah Pelaku Usaha Dalam Negeri atau Pelaku Usaha Luar Negeri yang menyediakan sarana komunikasi elektronik selain penyelenggara telekomunikasi yang hanya berfungsi sebagai perantara dalam komunikasi elektronik antara pengirim dan penerima.	
	Pasal 1 angka 12 Retail Online adalah Pedagang (*Merchant*) yang melakukan PMSE dengan sarana berupa situs web	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	atau aplikasi secara komersial yang dibuat, dikelola, dan/atau dimiliki sendiri.	
	Pasal 1 angka 13 Lokapasar (*Marketplace*) adalah penyedia sarana yang sebagian atau keseluruhan proses transaksi berada di dalam Sistem Elektronik berupa situs web atau aplikasi secara komersial sebagai wadah bagi Pedagang (*Merchant*) untuk dapat memasang penawaran Barang dan/atau Jasa.	
	Pasal 1 angka 15 Pelantar (*Platform*) Pembanding Harga adalah sarana untuk menjalankan Sistem Elektronik berupa situs web atau aplikasi dengan tujuan komersial yang menampilkan perbandingan harga Barang dan/atau Jasa yang dijual pada situs web atau aplikasi lain.	
	Pasal 1 angka 17 *Social-Commerce* adalah penyelenggara media sosial yang menyediakan fitur, menu, dan/atau fasilitas tertentu yang memungkinkan Pedagang	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(*Merchant*) dapat memasang penawaran Barang dan/atau Jasa.	
	Pasal 1 angka 18 Media Sosial adalah laman atau aplikasi yang memungkinkan pengguna dapat membuat dan berbagi isi atau terlibat dalam jaringan sosial.	
	Pasal 1 angka 24 Perizinan Berusaha Bidang PMSE adalah legalitas yang diberikan kepada Pelaku Usaha untuk memulai dan menjalankan usaha dan/atau kegiatan PMSE.	
	Pasal 1 angka 25 Surat Izin Usaha Perwakilan Perusahaan Perdagangan Asing di Bidang PMSE yang selanjutnya disebut SIUP3A Bidang PMSE adalah Perizinan Berusaha untuk melaksanakan kegiatan usaha perwakilan perusahaan Perdagangan asing di bidang PMSE.	
	Pasal 1 angka 26 Sistem Perizinan Berusaha Terintegrasi Secara Elektronik (*Online Single Submission*) yang	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	selanjutnya disebut Sistem OSS adalah sistem elektronik terintegrasi yang dikelola dan diselenggarakan oleh Lembaga Pengelola dan Penyelenggara *Online Single Submission* untuk penyelenggaraan Perizinan Berusaha berbasis risiko. Pasal 1 angka 28 Pemutusan Akses adalah tindakan pemblokiran akses, penutupan akun, dan/atau penghapusan konten.	
2	Pasal 3 (1) Pelaku Usaha wajib memiliki Perizinan Berusaha dalam melakukan kegiatan usaha di sektor Perdagangan sesuai dengan ketentuan peraturan perundang-undangan mengenai penyelenggaraan Perizinan Berusaha berbasis risiko. (2) Selain Perizinan Berusaha sebagaimana dimaksud pada ayat (1) Pelaku Usaha wajib memperoleh Perizinan Berusaha pada masing-masing sektor sesuai dengan ketentuan	Pasal *a quo* memberikan kewajiban bagi Pelaku Usaha untuk memiliki Perizinan Berusaha dalam melakukan kegiatan usaha di sektor perdagangan serta masing-masing sektor terkait. Oleh sebab itu, Aktor Perdagangan Elektronik yang juga merupakan PSE lingkup privat di bidang kegiatan perdagangan juga dibebani kewajiban pendaftaran sesuai aturan mengenai pendaftaran PSE. Ketentuan *a quo* sejalan dengan landasan hukum terkait PSE seperti PP 71/2019

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	peraturan perundang-undangan mengenai penyelenggaraan Perizinan Berusaha berbasis risiko. (3) PSP dikecualikan dari ketentuan kewajiban memiliki Perizinan Berusaha sebagaimana dimaksud pada ayat (1) jika: a. bukan merupakan pihak yang mendapatkan manfaat (*beneficiary*) secara langsung dari transaksi; atau b. tidak terlibat langsung dalam hubungan kontraktual para pihak yang melakukan PMSE.	dan PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021 yang mewajibkan PSE untuk melakukan pendaftaran.
3	Pasal 5 (1) Pedagang (*Merchant*) luar negeri yang melakukan kegiatan PMSE di PPMSE yang menyediakan sarana bagi Pedagang (Merchant) Luar Negeri wajib menyampaikan: a. identitas Pedagang (Merchant) luar negeri berupa nama dan	Ketentuan Pasal *a quo* membebani kewajiban bagi Pedagang luar negeri yang melakukan kegiatan PMSE di PPMSE Indonesia. Pasal *a quo* pada prinsipnya menghendaki agar setiap pedagang luar negeri di platform PSE dalam negeri untuk dibebani kewajiban-kewajiban

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	alamat negara asal Pedagang (Merchant) luar negeri; b. izin usaha yang dikeluarkan oleh lembaga yang berwenang di negara asal yang dilegalisasi oleh: 1. otoritas yang berkompeten bagi negara peserta Konvensi Penghapusan Persyaratan Legalisasi Terhadap Dokumen Publik Asing; atau 2. pejabat perwakilan Republik Indonesia di negara asal bagi negara bukan peserta Konvensi Penghapusan Persyaratan Legalisasi Terhadap Dokumen Publik Asing; a. bukti pemenuhan standar atau persyaratan teknis Barang dan/atau Jasa yang diwajibkan; dan b. nomor rekening bank yang digunakan untuk transaksi, kepada	administratif yang berkaitan dengan penyelenggaraan sistem elektronik di Indonesia. Kewajiban tersebut melingkupi kewajiban identitas pedagang, izin usaha dari negara asal, bukti pemenuhan standar barang, hingga nomor rekening. Selain itu, Pedagang luar negeri dibebani kewajiban untuk penggunaan bahasa Indonesia dan penayangan informasi asal negara. Tidak hanya itu PPMSE yang merupakan PSE lingkup privat juga diwajibkan untuk melakukan penyimpanan data dari Pedagang luar negeri tersebut.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	PPMSE dalam negeri yang menyediakan sarana bagi Pedagang (Merchant) luar negeri dimaksud. (2) Selain penyampaian persyaratan sebagaimana dimaksud pada ayat (1), Pedagang (*Merchant*) luar negeri dalam melakukan kegiatan PMSE di PPMSE yang menyediakan sarana bagi Pedagang (Merchant) Luar Negeri wajib: a. menggunakan Bahasa Indonesia yang mudah dimengerti pada deskripsi Barang dan/atau Jasa yang diperdagangkan; dan b. menayangkan informasi negara asal pengiriman Barang dan/atau Jasa. (3) Pemenuhan persyaratan sebagaimana dimaksud pada ayat (1) huruf a dan huruf b harus dilengkapi dengan	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sertifikat atau laporan hasil inspeksi terhadap kebenaran data yang diterbitkan oleh lembaga survei independen di negara asal. (4) Bukti pemenuhan standar Barang dan/atau Jasa sebagaimana dimaksud pada ayat (1) huruf c berupa: a. pemenuhan Standar Nasional Indonesia atau persyaratan teknis lain bagi Barang dan/atau Jasa yang telah diberlakukan Standar Nasional Indonesia atau persyaratan teknis secara wajib sesuai dengan ketentuan peraturan perundang-undangan; b. pemenuhan standar atau persyaratan teknis di negara asal bagi Barang dan/atau Jasa yang belum diberlakukan Standar Nasional Indonesia	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	atau persyaratan teknis secara wajib; dan c. sertifikat halal bagi Barang dan/atau Jasa yang wajib bersertifikat halal sesuai dengan ketentuan peraturan perundang-undangan. (5) Dalam hal Pedagang (*Merchant*) luar negeri tidak memenuhi ketentuan sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3), PPMSE yang menyediakan sarana bagi Pedagang (*Merchant*) Luar Negeri wajib menolak permintaan pendaftaran Pedagang (*Merchant*) luar negeri dimaksud. (6) PPMSE memfasilitasi Pedagang (*Merchant*) luar negeri wajib melakukan penyimpanan data Pedagang (*Merchant*) luar negeri yang didaftarkan pada sarana PMSE yang dimiliki.	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
4	Pasal 7 (1) Untuk memperoleh Perizinan Berusaha Bidang PMSE, PPMSE dalam negeri dan PSP yang tidak dikecualikan dari ketentuan kewajiban memiliki Perizinan Berusaha sebagaimana dimaksud dalam Pasal 6 mengajukan permohonan kepada Menteri melalui Lembaga OSS. (2) Permohonan sebagaimana dimaksud pada ayat (1) harus memenuhi persyaratan sesuai dengan ketentuan peraturan perundang-undangan mengenai penyelenggaraan Perizinan Berusaha berbasis risiko. (3) Perizinan Berusaha Bidang PMSE sebagaimana dimaksud pada ayat (1) diterbitkan oleh Lembaga OSS untuk dan atas nama Menteri. (4) Perizinan Berusaha Bidang PMSE berlaku selama PPMSE dalam negeri dan PSP yang tidak dikecualikan sebagaimana	Pasal *a quo* mengatur mengenai kewajiban Perizinan Berusaha bagi PSE berupa PPMSE dalam negeri dan PSP, yang diajukan kepada Menteri Perdagangan melalui Lembaga OSS. Pengajuan tersebut dilakukan sesuai penyelenggaraan perizinan berusaha berbasis risiko yang nantinya diterbitkan oleh Lembaga OSS untuk dan atas nama Menteri Perdagangan.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	dimaksud pada ayat (1) menjalankan kegiatan usaha dan/atau kegiatannya.	
5	Pasal 8 Perizinan Berusaha bagi PPMSE dalam negeri, menggunakan klasifikasi baku lapangan usaha Indonesia bagi portal web dan/atau platform digital dengan tujuan komersial.	Pasal *a quo* menghendaki agar Perizinan Berusaha bagi PSE privat berupa PPMSE dalam negeri untuk menggunakan nomor KBLI untuk portal web dan/atau platform digital dengan tujuan komersial, sebagaimana telah diatur dalam peraturan perundang-undangan terkait PSE tersebut.
6	Pasal 9 (1) PPMSE dan PSP yang tidak dikecualikan dari ketentuan kewajiban memiliki Perizinan Berusaha sebagaimana dimaksud dalam Pasal 3 ayat (3) wajib memiliki layanan pengaduan Konsumen sesuai dengan persyaratan berdasarkan ketentuan peraturan perundang-undangan mengenai penyelenggaraan Perizinan Berusaha berbasis risiko.	Ketentuan Pasal *a quo* membebani kewajiban bagi PSE berupa PPMSE dan PSE untuk memiliki layanan pengaduan konsumen, yang termuat dalam laman yang dibaca konsumen serta memuat nomor kontak dan/atau alamat surat elektronik yang wajib dihubungi dan ditanggapi.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(2) Layanan pengaduan Konsumen sebagaimana dimaksud pada ayat (1) wajib ditampilkan dengan jelas pada laman yang mudah dibaca oleh Konsumen. (3) Layanan pengaduan Konsumen sebagaimana dimaksud pada ayat (1) berupa nomor kontak dan/atau alamat surat elektronik yang wajib dapat dihubungi dan ditanggapi.	
7	Pasal 10 Selain layanan pengaduan Konsumen sebagaimana dimaksud dalam Pasal 9, PPMSE dan PSP yang tidak dikecualikan dari ketentuan kewajiban memiliki Perizinan Berusaha sebagaimana dimaksud dalam Pasal 3 ayat (3) wajib menayangkan informasi kontak layanan pengaduan Konsumen Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga yang ditampilkan dengan jelas pada laman yang mudah dibaca oleh Konsumen.	Ketentuan Pasal *a quo* mewajibkan bagi PSE berupa PPMSE dan PSP untuk menayangkan informasi kontak layanan pengaduan konsumen Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga yang ditampilkan secara jelas pada laman yang mudah dibaca konsumen.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
8	Pasal 11 (1) Pedagang (Merchant) wajib menayangkan informasi mengenai bukti pemenuhan standar Barang dan/atau Jasa, berupa: a. nomor pendaftaran barang atau sertifikat Standar Nasional Indonesia atau persyaratan teknis lain bagi Barang dan/atau Jasa yang telah diberlakukan Standar Nasional Indonesia atau persyaratan teknis wajib sesuai dengan ketentuan peraturan perundang-undangan; b. nomor sertifikat halal bagi Barang dan/atau Jasa yang wajib bersertifikat halal sesuai dengan ketentuan peraturan perundang-undangan;	Ketentuan Pasal *a quo* mengamanatkan bagi Pedagang dalam suatu platform PSE perdagangan elektronik untuk diwajibkan menayangkan informasi mengenai bukti pemenuhan standar Barang dan/atau Jasa, sebagaimana termuat dari huruf a sampai dengan huruf d. Selain itu, terdapat kewajiban berupa fasilitasi dan penayangan informasi mengenai asal Pedagang (*Merchant*) luar negeri, negara asal pengiriman Barang asal luar negeri, dan bukti pemenuhan standar Barang dan/atau Jasa.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	c. nomor registrasi produk Barang terkait keamanan, keselamatan, kesehatan, dan lingkungan hidup untuk Barang yang diwajibkan sesuai dengan ketentuan peraturan perundang-undangan; dan d. nomor izin, nomor registrasi, atau nomor sertifikat untuk produk kosmetik, obat, dan makanan sesuai dengan ketentuan peraturan perundang-undangan, (2) PPMSE wajib memfasilitasi dan menayangkan informasi negara asal Pedagang (*Merchant*) luar negeri, negara asal pengiriman Barang asal luar negeri, dan bukti pemenuhan standar Barang dan/atau Jasa sebagaimana dimaksud pada ayat (1).	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
9	Pasal 12 (1) PPMSE harus berperan aktif dalam pemenuhan persyaratan Perizinan Berusaha bagi Pedagang (*Merchant*) dalam negeri dan Pedagang (*Merchant*) luar negeri. (2) Peran aktif dalam pemenuhan persyaratan Perizinan Berusaha sebagaimana dimaksud pada ayat (1) dilaksanakan dalam bentuk: a. penyediaan fitur Perizinan Berusaha dalam proses pendaftaran Pedagang (*Merchant*) pada Sistem Elektronik; b. penyediaan tautan pendaftaran Perizinan Berusaha yang terhubung langsung pada Sistem OSS; dan/atau c. pelaksanaan sosialisasi bagi Pedagang (*Merchant*)	Pasal *a quo* menghendaki adanya peran aktif bagi PSE berupa PPMSE untuk membantu pemenuhan persyaratan Perizinan Berusaha bagi Pedagang dalam negeri maupun luar negeri. Pemenuhan tersebut dilaksanakan dengan bentuk penyediaan fitur perizinan pada Sistem Elektronik, penyediaan tautan pendaftaran Perizinan Berusaha yang tersambung dengan Sistem OSS; dan pelaksanaan sosialisasi.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	untuk mendaftarkan usahanya.	
1.	Pasal 14 PPMSE yang menyediakan sarana komunikasi elektronik bagi Pedagang (*Merchant*) harus menyediakan fasilitas yang menginformasikan dan/atau menghubungkan ke laman Lembaga OSS.	Pasal *a quo* menghendaki agar PSE berupa PPSME yang menyediakan sarana komunikasi elektronik bagi Pedagang untuk tersambung ke laman OSS dalam konteks perizinan berusaha.
2.	Pasal 17 PPMSE wajib menyampaikan data dan/atau informasi kepada lembaga pemerintah non kementerian yang menyelenggarakan urusan pemerintahan di bidang statistik sesuai dengan ketentuan peraturan perundang-undangan.	Pasal *a quo* menghendaki agar PSE berupa PMSE untuk membagikan data dan/atau informasi kepada lembaga pemerintah non kementerian yang menyelenggarakan urusan pemerintahan di bidang statistik.
3.	Pasal 18 ayat (1) PPMSE luar negeri sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b yang memenuhi kriteria tertentu, wajib menunjuk perwakilan yang berkedudukan di wilayah hukum Negara Kesatuan Republik Indonesia yang dapat bertindak	Pasal *a quo* menghendaki agar PSE berupa PPMSE yang berasal dari luar negeri untuk diwajibkan menunjuk perwakilan berkedudukan di wilayah hukum NKRI.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sebagai dan atas nama PPMSE dimaksud.	
4.	Pasal 26 Dalam hal Iklan Elektronik disampaikan melalui sarana PPMSE, PPMSE wajib mematuhi ketentuan peraturan perundang-undangan di bidang penyiaran, perlindungan atas privasi dan data pribadi, perlindungan Konsumen, dan tidak bertentangan dengan prinsip persaingan usaha yang sehat.	Pasal *a quo* mengatur mengenai kewajiban bagi iklan elektronik melalui PPMSE sebagai PSE untuk mengikuti ketentuan peraturan di bidang penyiaran, perlindungan privasi dan data pribadi, perlindungan konsumen, dan memperhatikan prinsip persaingan usaha yang sehat.

Sumber: diolah Penulis (2026).

4. Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik

Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik (PM Komdigi 5/2025) merupakan tindak lanjut beberapa ketentuan dalam PP 71/2019. Cakupan lingkup publik dalam PM Komdigi 5/2025 meliputi instansi dan lembaga publik, dengan mengecualikan otoritas pengatur serta pengawas di sektor keuangan. Selaras dengan PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021, orientasi pengaturan dalam PM Komdigi 5/2025 menitikberatkan pada kewajiban pendaftaran PSE guna menjamin penyelenggaraan sistem elektronik yang andal, aman, dan bertanggung jawab."

Terdapat beberapa materi muatan dalam PM Komdigi 5/2025 yang memiliki keterkaitan dengan penyelenggaraan sistem elektronik di Indonesia. Keterkaitan tersebut dipetakan dalam tabel sebagai berikut:

Tabel 3. 10. Pemetaan Ketentuan dalam PM Komdigi 5/2025 yang berkaitan dengan PSE

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 1 Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	Definisi-definisi yang terdapat dalam Pasal 1 memberikan landasan definisi kuat bagi PSE lingkup publik khususnya kepada instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara. Lebih lanjut, PSE lingkup publik *user generated content* juga didefinisikan sebagai PSE yang penyediaan, penayanangan, pengunggahan, dan/atau pertukaran informasinya dilakukan oleh pengguna Sistem Elektronik.
	Pasal 1 angka 2 Penyelenggara Sistem Elektronik Lingkup Publik yang selanjutnya disebut PSE Lingkup Publik adalah Penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau Institusi yang ditunjuk oleh Instansi Penyelenggara Negara	
	Pasal 1 angka 3 PSE Lingkup Publik User Generated Content adalah PSE Lingkup Publik	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	yang penyediaan, penayangan, pengunggahan, dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektroniknya dilakukan oleh Pengguna Sistem Elektronik.	
2	Pasal 3 (1) PSE Lingkup Publik meliputi: a. Instansi; dan b. Institusi. (2) PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) tidak termasuk PSE Lingkup Publik yang merupakan otoritas pengatur dan pengawas sektor keuangan. (3) Institusi sebagaimana dimaksud pada ayat (1) huruf b paling sedikit harus memenuhi kriteria: a. memiliki tanda daftar Penyelenggara Sistem Elektronik Lingkup Privat sesuai peraturan perundang-undangan; b. berbentuk badan hukum Indonesia; dan	Pasal *a quo* memberikan kedudukan bahwa jenis PSE lingkup publik yang mencakup instansi maupun institusi dengan pengecualian kepada PSE Lingkup publik yang bergerak/merupakan otoritas pengatur dan pengawas sektor keuangan. Pengecualian ini semata-mata diberikan untuk menjaga dan melindungi PSE Lingkup Publik pada sektor keuangan yang telah memiliki pengaturan tersendiri

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	c. memiliki pusat data yang berlokasi di wilayah Negara Kesatuan Republik Indonesia. (4) Penunjukan Institusi sebagaimana dimaksud pada ayat (1) huruf b merupakan penugasan yang ditetapkan dengan peraturan perundang-undangan.	
3	Pasal 4 (1) Setiap PSE Lingkup Publik wajib melakukan pendaftaran PSE Lingkup Publik terhadap Sistem Elektronik yang diselenggarakannya. (2) Kewajiban pendaftaran PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) dilakukan sebelum Sistem Elektronik mulai digunakan oleh Pengguna Sistem Elektronik. (3) Selain kewajiban melakukan pendaftaran sebagaimana dimaksud pada ayat (1), PSE Lingkup Publik wajib: a. menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan	Pasal *a quo* merupakan jaminan perlindungan hukum yang diberikan melalui pendaftaran PSE Lingkup Publik sehingga keandalan dan keamanan PSE Lingkup Publik dapat dipertanggungjawabkan. Pendaftaran PSE Lingkup Publik dilakukan kepada Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian; b. melakukan pelindungan Data Pribadi; dan c. melakukan uji kelaikan Sistem Elektronik, sesuai dengan ketentuan peraturan perundangundangan. (4) Pendaftaran PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) diajukan kepada Menteri melalui layanan pendaftaran secara elektronik.	
4	Pasal 5 (1) PSE Lingkup Publik harus menunjuk pejabat pendaftar PSE Lingkup Publik. (2) Pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) merupakan pejabat pendaftar yang berasal dari: a. Instansi; atau b. Institusi.	Pasal *a quo* menjelaskan keberadaan pejabat pendaftar PSE Lingkup publik yang merupakan "penanggung jawab" PSE yang melakukan pendaftaran tersebut

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
5	Pasal 16 (1) Menteri mengenakan sanksi administratif kepada PSE Lingkup Publik yang: a. tidak melakukan pendaftaran PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 4 ayat (1); b. tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 4 ayat (3); dan/atau c. telah mempunyai tanda daftar tetapi tidak melaporkan perubahan informasi pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 14 ayat (1). (2) Pengenaan sanksi administratif sebagaimana dimaksud pada ayat (1) dilakukan melalui koordinasi dengan pimpinan Kementerian atau Lembaga terkait.	Pasal *a quo* menjelaskan kewenangan Menteri untuk mengenakan sanksi administratif kepada PSE yang tidak melakukan pendaftaran, tidak memenuhi kewajiban, hingga telah mempunyai tanda daftar tetapi tidak melaporkan perubahan informasi.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(3) Dalam hal PSE Lingkup Publik tidak melakukan pendaftaran sebagaimana dimaksud pada ayat (1) huruf a, Menteri mengenakan sanksi administratif berupa Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik (access blocking). (4) [...]	

Sumber: diolah Penulis (2026).

D. Kebijakan dan Rancangan Peraturan Terkait pp 71/2019

Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (RPP PDP) merupakan regulasi turunan dari UU 27/2022. Penyusunan RPP PDP bertujuan untuk memberikan penjabaran teknis atas UU 27/2022, sebagaimana dimandatkan oleh undang-undang tersebut Salah satu fokus utamanya adalah mengenai kelembagaan Otoritas Pelindungan Data Pribadi yang akan menyelenggarakan serta mengoordinasikan upaya pelindungan data pribadi di Indonesia. Saat ini, proses tersebut masih dalam masa transisi hingga RPP *a quo* resmi disahkan oleh Pemerintah.

Terdapat beberapa materi muatan dalam RPP PDP yang memiliki keterkaitan dengan penyelenggaraan sistem elektronik di Indonesia. Keterkaitan tersebut telah dipetakan dalam tabel sebagai berikut:

Tabel 3. 11. Pemetaan Ketentuan dalam RPP PDP yang berkaitan dengan pelindungan data pribadi dalam PSE.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
1	Pasal 1 angka 1 Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.	Sebagaimana aturan dalam UU 27/2022, PSE Lingkup Privat merupakan salah satu subjek dari pelindungan data pribadi. Oleh sebab itu, terdapat beberapa definisi nomenklatur dalam RPP *a quo* yang berkaitan dengan data pribadi, maupun pelindungan data pribadi. Lebih lanjut, dalam menjalankan fungsinya, PSE Lingkup Privat melakukan pengendalian maupun pemrosesan data pribadi. Aktivitas tersebut menempatkan PSE Lingkup Privat sebagai Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, bergantung pada peran dan tanggung jawabnya dalam sistem elektronik yang dikelola.
	Pasal 1 angka 2 Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.	
	Pasal 1 angka 4 Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.	
	Pasal 1 angka 5 Prosesor Data Pribadi adalah setiap orang, badan publik, dan organisasi	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.	
2	Pasal 5 Elemen Data Pribadi terdiri dari: a. data tentang orang perseorangan; b. dapat mengidentifikasi seseorang secara tersendiri atau dikombinasikan dengan data lainnya; dan c. dapat mengidentifikasi secara langsung maupun tidak langsung melalui sistem elektronik dan nonelektronik.	Pasal *a quo* menegaskan bahwa data dalam sistem elektronik yang dikelola oleh PSE Lingkup Privat merupakan objek pelindungan data pribadi yang menjadi fokus pengaturan dalam RPP ini.
3	Pasal 9 Pemrosesan Data Pribadi meliputi: a. pemerolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau	Pasal 9 sampai dengan Pasal 15 RPP PDP mengatur siklus pemrosesan data pribadi oleh PSE Lingkup Privat yang mencakup tahap perolehan, pengumpulan, hingga pemusnahan. Mengingat tahapan tersebut dijabarkan secara rinci dalam Pasal 10 hingga

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	f. penghapusan atau pemusnahan.	Pasal 15, PSE berkewajiban menyelaraskan tata kelola data internalnya dengan ketentuan pemrosesan yang ditetapkan dalam RPP *a quo*.
4	Pasal 10 Dalam rangka pemerolehan dan pengumpulan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf a, Pengendali Data Pribadi harus: a. menentukan dasar pemrosesan sebelum melakukan pemerolehan dan pengumpulan Data Pribadi; b. menentukan secara jelas tujuan dari pemerolehan dan pengumpulan Data Pribadi, dengan mempertimbangkan kepentingan Subjek Data Pribadi; c. membatasi besaran Data Pribadi yang dikumpulkan berdasarkan tujuan yang telah ditentukan; d. menentukan mekanisme yang aman dalam pemerolehan dan pengumpulan Data Pribadi; e. memberikan informasi terkait tujuan pemrosesan sebelum dilakukan pemerolehan dan pengumpulan Data Pribadi; dan	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	f. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal pemerolehan dan pengumpulan Data Pribadi sesuai ketentuan peraturan perundang-undangan.	
5	Pasal 11 Dalam rangka pengolahan dan penganalisisan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf b, Pengendali Data Pribadi harus: a. menentukan mekanisme dan/atau standar penerapan kualitas data untuk memastikan bahwa Data Pribadi yang diolah dan dianalisis telah akurat dan lengkap; b. memberikan informasi kepada Subjek Data Pribadi jika terdapat pengolahan dan penganalisisan Data Pribadi di luar atau sebagai tambahan tujuan dari tujuan awal pengolahan dan penganalisisan Data Pribadi; c. melakukan penilaian dampak Pelindungan Data Pribadi untuk pengolahan dan penganalisisan Data Pribadi yang memiliki	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	potensi risiko tinggi terhadap Subjek Data Pribadi; d. memfasilitasi hak Subjek Data Pribadi untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis; dan e. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal pengolahan dan penganalisisan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.	
6	Pasal 12 Dalam rangka penyimpanan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf c, Pengendali Data Pribadi harus: a. menentukan dan menerapkan pengendalian keamanan Data Pribadi yang disimpan baik secara fisik maupun elektronik; b. menetapkan dan menerapkan mekanisme retensi Data Pribadi;	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	c. menentukan masa retensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; d. menerapkan pencegahan kegagalan Pelindungan Data Pribadi dalam hal penyimpanan Data Pribadi dengan: 1. menerapkan enkripsi dan/atau penyamaran data; 2. membuat salinan cadangan terhadap Data Pribadi; dan 3. melakukan enkripsi dan/atau penyamaran data terhadap salinan cadangan Data Pribadi. e. membatasi pihak-pihak yang dapat mengakses Data Pribadi; f. mengetahui, mencatat dan/ mendokumentasikan lokasi penyimpanan, dan media penyimpanan Data Pribadi; dan g. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal penyimpanan Data Pribadi	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sesuai dengan ketentuan peraturan perundang-undangan.	
7	Pasal 13 Dalam rangka perbaikan dan pembaruan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf d, Pengendali Data Pribadi harus: a. memfasilitasi Subjek Data Pribadi untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi; b. melakukan verifikasi Data Pribadi dari Subjek Data Pribadi; dan c. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal perbaikan dan pembaruan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.	
8	Pasal 14 Dalam rangka penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf e, Pengendali Data Pribadi harus:	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	a. memiliki dasar pemrosesan Data Pribadi sebelum menampilkan, mengumumkan, mentransfer, menyebarluaskan atau mengungkap Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; b. mematuhi kriteria transfer Data Pribadi ke luar wilayah hukum Negara Republik Indonesia sebagaimana diatur dalam ketentuan peraturan perundang-undangan; c. menerapkan pengendalian keamanan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; d. membatasi pengungkapan Data Pribadi sesuai tujuan pemrosesan yang telah ditentukan dan disetujui oleh Subjek Data Pribadi, serta tidak bertentangan dengan peraturan perundang-undangan; dan e. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal penampilan, pengumuman, transfer, penyebarluasan, atau	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	pengungkapan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.	
9	Pasal 15 Dalam rangka penghapusan atau pemusnahan Data Pribadi sebagaimana dimaksud dalam Pasal 9 huruf f, Pengendali Data Pribadi harus: a. menghapus atau memusnahkan Data Pribadi kecuali dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan; b. menerapkan mekanisme penghapusan atau pemusnahan Data Pribadi yang aman; c. memfasilitasi pemenuhan hak Subjek Data Pribadi untuk melakukan penghapusan data, sepanjang tidak bertentangan dengan ketentuan peraturan perundang-undangan; d. melakukan tindakan dalam permintaan Subjek Data Pribadi untuk menghapus Data Pribadi valid/sah dan tidak bertentangan dengan ketentuan peraturan perundang-undangan, dengan:	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	1. melakukan penghapusan atau pemusnahan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; 2. melakukan penghapusan atau pemusnahan Data Pribadi di semua lokasi penyimpanan Data Pribadi; 3. menyimpan bukti penghapusan atau pemusnahan Data Pribadi dalam bentuk berita acara penghapusan; dan 4. menyampaikan bukti penghapusan atau pemusnahan Data Pribadi kepada Subjek Data Pribadi; dan e. menerapkan prinsip-prinsip pemrosesan Data Pribadi dalam hal penghapusan atau pemusnahan Data Pribadi sesuai ketentuan peraturan perundang-undangan.	
10	Pasal 142	Pasal *a quo* mewajibkan PSE yang merupakan Pengendali Data Pribadi mencegah terjadinya akses

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	(1) Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah. (2) Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan menggunakan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab. (3) Pencegahan sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.	tidak sah terhadap Data Pribadi. Pencegahan tersebut dilakukan melalui penerapan sistem keamanan data pribadi yang andal, aman, dan bertanggung jawab. Seluruh proses pencegahan dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
11	Pasal 161 (1) Prosesor Data Pribadi wajib melindungi Data Pribadi dari pemrosesan yang tidak sah. (2) Prosesor Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah. (3) Pencegahan sebagaimana dimaksud pada ayat (2) dilakukan dengan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi	Pasal *a quo* mengatur kewajiban Prosesor Data Pribadi untuk melindungi Data Pribadi dari pemrosesan dan akses yang tidak sah. Pencegahan dilakukan dengan sistem keamanan yang andal sesuai dengan ketentuan peraturan perundang-undangan.

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	sistem elektronik secara andal, aman, dan bertanggung jawab. (4) Pencegahan sebagaimana dimaksud pada ayat (3) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.	
12	Pasal 200 huruf n Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 199 ayat (2), Lembaga PDP berwenang: [...] n. melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga; dan	
13	Pasal 219 ayat (3) Dalam rangka melakukan pemeriksaan lanjutan sebagaimana dimaksud pada ayat (1), Lembaga PDP dapat: a. mendengarkan keterangan saksi, ahli, dan/atau pihak lain yang	

No.	Ketentuan dan Bunyi Pasal	Keterkaitan
	terkait dengan pemrosesan Data Pribadi; b. melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi; c. memperoleh akses terhadap Data Pribadi yang diproses Pengendali Data Pribadi dan/atau Prosesor Data Pribadi; d. menunjuk pihak ketiga untuk melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi; dan/atau e. melakukan tindakan dalam rangka menjalankan kewenangan sesuai dengan ketentuan peraturan perundang-undangan.	

Sumber: diolah Penulis (2026).

BAB IV
USULAN JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP PENGEMBANGAN PENGATURAN PENYELENGGARA SISTEM ELEKTRONIK

BAB IV
USULAN JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP PENGEMBANGAN PENGATURAN PENYELENGGARA SISTEM ELEKTRONIK

A. Sasaran

Sasaran pengaturan dalam Revisi PP 71/2019 adalah untuk memberikan kepastian hukum atas perkembangan administrasi PSE, penguatan pelindungan data, serta pelindungan anak dalam ruang digital. Revisi PP 71/2019 dimaksudkan untuk menjalankan amanat UU 27/2022 dan UU 1/2024, serta mengangkat materi muatan terkait PSE lingkup privat yang diatur dalam PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021. Lebih spesifik dalam konteks proses administrasi PSE, Revisi PP 71/2019 mengadopsi ketentuan dalam PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021 dalam hal pengaturan pendaftaran, tata kelola, moderasi terhadap informasi atau dokumen elektronik, hingga penegakan hukum terhadap PSE. Selain itu, Revisi PP 71/2019 mengarah kepada adopsi terhadap ketentuan pelindungan data pribadi dalam kaitannya dengan penyelenggaraan sistem elektronik yang terdapat dalam UU 27/2022 beserta aturan turunannya. Tidak hanya itu, Revisi PP 71/2019 juga mengadopsi ketentuan pelindungan anak di ranah penyelenggaraan sistem elektronik sebagai salah satu amanat dari UU 1/2024. Dengan demikian, materi muatan dalam Revisi PP 71/2019 akan memberikan kepastian hukum bagi proses bisnis PSE lingkup privat; memberikan perlindungan hukum atas data pribadi yang tersimpan dan dikelola oleh PSE; serta mengintegrasikan perspektif perlindungan bagi anak dalam penyelenggaraan sistem elektronik.

B. Arah Pengaturan

Arah pengaturan dari Revisi PP 71/2019 adalah menyesuaikan perkembangan dalam pengaturan PSE dengan mengadopsi pengaturan terkait

pendaftaran dan tata kelola PSE, mengadopsi ketentuan mengenai pelindungan data pribadi dalam penyelenggaraan sistem elektronik, serta menambahkan pengaturan mengenai pelindungan anak dalam penyelenggaraan sistem elektronik.

C. Jangkauan Pengaturan

Jangkauan subjek pengaturan Revisi PP 71/2019 mencakup seluruh PSE publik dan privat, baik yang berasal dari dalam maupun luar negeri, yang beroperasi di wilayah Indonesia. Selain itu, cakupan regulasi ini meluas hingga ke pengguna serta pihak-pihak terkait dalam ekosistem penyelenggaraan sistem elektronik nasional.

Ruang lingkup objek pengaturan dalam Revisi PP 71/2019 adalah penambahan norma-norma terkait PSE, khususnya yang berkaitan dengan materi muatan dalam peraturan perundang-undangan terkait yang terbit dalam kurun waktu tahun 2019 hingga saat ini. Penambahan norma tersebut meliputi: *pertama,* pengaturan mengenai pendaftaran, tata kelola, hingga mekanisme penegakan hukum dalam administrasi registrasi PSE dan perizinan berusaha di Indonesia; *kedua,* pengaturan terkait pelindungan data pribadi dalam proses bisnis PSE serta hak dan kewajiban dari pihak-pihak yang terlibat; dan *ketiga,* pengaturan mengenai pelindungan terhadap anak dalam penyelenggaraan sistem elektronik. Selain itu, Revisi PP 71/2019 diarahkan untuk memperbarui norma penyelenggaraan sistem elektronik dengan mengacu pada standar internasional, seperti *EU Digital Services Act*. Langkah ini dilakukan untuk menyempurnakan tata kelola PSE, khususnya dalam hal perlindungan hak pengguna, penanganan konten ilegal, serta transparansi periklanan digital. Di samping itu, revisi ini juga mendorong mekanisme moderasi konten yang lebih transparan dan inklusif dengan mengedepankan partisipasi aktif pengguna.

D. Ruang Lingkup Materi Pengaturan

Ruang lingkup Revisi PP 71/2019 meliputi penyesuaian dan penambahan norma terkait penyelenggaraan sistem dan transaksi elektronik guna memperbarui ketentuan dalam PP 71/2019, dengan rincian sebagai berikut:

1) Penambahan dan penyesuaian terhadap definisi-definisi dari nomenklatur yang berkaitan dengan norma-norma baru terkait PSE;

2) Penambahan satu bab tersendiri, berisi norma pengaturan yang berkaitan dengan pendaftaran, tata cara, serta tata kelola bagi PSE lingkup privat—yang selama ini diatur dalam PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021;

3) Perubahan teknis mengenai tata kelola PSE untuk disesuaikan dengan mempertimbangkan konsep dan materi muatan yang terdapat dalam beberapa aturan hukum di tingkat internasional. Aturan hukum yang dapat menjadi pertimbangan tersebut sebagaimana telah disebutkan dalam sub bab mengenai perbandingan antar negara, misalnya *EU Digital Service Act* Uni Eropa dan Tiongkok yang mengatur PSE sebagai bagian dari rezim hukum keamanan siber. Berdasarkan komparasi tersebut, maka revisi PP 71/2019 dapat mengadopsi dan mengakomodasi sejumlah materi muatan yang sekiranya mendukung penyelenggaraan PSE di Indonesia. Sejumlah materi muatan tersebut meliputi mekanisme perlindungan terhadap hak pengguna, moderasi konten, perlindungan terhadap konten ilegal serta ancaman siber, dan pengaturan mengenai iklan dalam PSE;

4) Akomodasi terhadap peraturan-peraturan yang memiliki keterkaitan dengan PSE dalam berbagai tingkat peraturan perundang-undangan, misalnya dalam konteks pelindungan data pribadi (yang diatur dalam UU 27/2022 dan nantinya RPP PDP) dan pelindungan terhadap anak dalam penyelenggaraan sistem elektronik (sebagaimana akan diatur dalam PP tersendiri). Materi muatan revisi PP 71/2019 perlu mengadopsi pengaturan-pengaturan di ranah tersebut;

5) Melakukan perbaikan terhadap aturan-aturan PSE yang bersifat "kontroversial." Perbaikan dilakukan dengan, antara lain, mengubah paradigma moderasi konten dengan menambah ruang partisipasi publik/pengguna; mengubah mekanisme pengenaan sanksi dalam administrasi PSE yang tidak merugikan pihak-pihak secara meluas, hingga mengedepankan transparansi dan akuntabilitas dalam penyelesaian aduan atau sengketa terkait PSE; serta

6) Penambahan Bagian Ketentuan Peralihan, guna menjamin sinkronisasi dengan peraturan perundang-undangan sektoral terkait penyelenggaraan sistem elektronik, seperti di bidang kesehatan, perdagangan melalui sistem elektronik, dan jurnalisme digital.

BAB V

PENUTUP

BAB V
PENUTUP

A. Kesimpulan

Seluruh analisis terhadap berbagai aspek dalam Naskah Urgensi ini dapat dirangkum ke dalam beberapa kesimpulan berikut:

1) Urgensi perubahan PP 71/2019 dilatarbelakangi oleh perkembangan yuridis dan dinamika empiris dalam penyelenggaraan sistem elektronik, khususnya terkait tata kelola PSE. Secara yuridis, lahirnya UU 27/2022 dan UU 1/2024 serta sejumlah regulasi tingkat menteri, seperti PM Kominfo 5/2020 jo. 10/2021 dan PM Komdigi 5/2025, menuntut adanya sinkronisasi norma. Revisi ini dimaksudkan untuk mengangkat materi muatan yang bersifat umum ke tingkat Peraturan Pemerintah guna memperkuat legalitasnya sebagai aturan pelaksana dari UU 1/2024. Secara empiris, berbagai tantangan praktis seperti kerumitan registrasi, moderasi konten, hingga urgensi pelindungan data pribadi menjadi alasan krusial bagi pemerintah untuk segera memperbarui ketentuan dalam PP 71/2019.

2) Pengaturan eksisting dalam PP 71/2019 telah mendefinisikan PSE secara luas sebagai entitas yang menyelenggarakan sistem elektronik dari tahap penyediaan hingga operasional. Saat ini, PSE diklasifikasikan berdasarkan asal (dalam negeri dan luar negeri) serta ruang lingkup (publik dan privat). Luasnya cakupan tersebut menuntut adanya pengaturan yang lebih spesifik dan relevan dengan karakteristik teknis serta risiko dari masing-masing kategori PSE guna menjamin kepastian hukum.

3) Perbandingan terhadap berbagai negara-negara yang telah mengatur PSE seperti Uni Eropa (dalam ranah negara multinasional), Republik Rakyat Tiongkok, dan Jepang, menunjukkan bahwa negara-

negara tersebut memberlakukan produk regulasi yang mengatur PSE secara komprehensif. Makna dari komprehensif tersebut adalah pengaturan PSE tidak hanya melingkupi aspek tata kelola PSE, tetapi juga mengatur pelindungan data pribadi, mekanisme mitigasi ancaman siber, peran serta negara, hingga bahkan penyelesaian sengketa antara pengguna/konsumen dengan PSE. Oleh sebab itu, aturan dari negara-negara misalnya *Digital Service Act* milik Uni Eropa dapat menjadi: a) panduan konkret bagi Pemerintah Indonesia apabila hendak mengatur ekosistem PSE melalui Revisi dari PP 71/2019; dan b) acuan dalam penyusunan norma berkaitan dengan perkembangan terhadap PSE.

4) Analisis terhadap peraturan perundang-undangan maupun hukum yang dicita-citakan (*lex constituendum*) di Indonesia sebetulnya telah menunjukkan adanya urgensi untuk merevisi PP 71/2019. Hal tersebut tercermin dalam peraturan perundang-undangan yang bersifat horizontal atau mengatur hal-hal terkait penyelenggaraan sistem dan transaksi elektronik—misalnya UU 11/2008 *jo.* UU 1 Tahun 2024, PM Kominfo 5/2020 *jo.* PM Kominfo 10/2021, dan PM Kominfo 3/2021. Peraturan perundang-undangan horizontal tersebut menunjukkan adanya aturan hukum sebagai bentuk adaptasi dan perkembangan terhadap penyelenggaraan dan tata kelola PSE di Indonesia. Selain itu, peraturan perundang-undangan vertikal dan sektoral juga menunjukkan telah terdapat berbagai aturan khusus dalam penyelenggaraan PSE di tiap-tiap sektor, misalnya dalam sektor perdagangan melalui sistem elektronik, kesehatan, dan bahkan jurnalisme digital. Terakhir, *lex constituendum* dalam RPP PDP maupun RPP Pelindungan Anak dalam PSE juga menghendaki adanya perubahan untuk mengakomodasi isu pelindungan data pribadi dan pelindungan anak dalam PSE dalam aturan khusus PSE—sebagaimana materi muatan dalam Revisi PP 71/2019.

5) Perubahan terhadap PP 71/2019 diperlukan guna memberikan jaminan dan kepastian hukum bagi pelaku usaha maupun pengguna dalam penyelenggaraan sistem elektronik. Oleh sebab itu, kebijakan untuk merevisi PP 71/2019 dengan menyesuaikan norma-norma di dalamnya menjadi upaya penting untuk membenahi tata kelola penyelenggaraan sistem dan transaksi elektronik. Adapun hal-hal yang perlu diperhatikan dalam arah, sasaran, dan materi muatan revisi PP 71/2019 meliputi: (a) perkembangan dalam penyelenggaraan sistem dan transaksi elektronik pasca-terbitnya UU 1/2024; (b) penjabaran aturan mengenai pelindungan data pribadi dalam PSE sesuai UU 27/2022 dan peraturan turunannya; (c) mengakomodasi ruang bagi pengaturan pelindungan anak dalam PSE sesuai amanat UU 1/2024; (d) mengakomodasi aturan teknis mengenai registrasi, tata kelola, hingga mekanisme penegakan hukum terhadap PSE lingkup privat yang selama ini diatur dalam PM Kominfo 5/2020 jo. PM Kominfo 10/2021; (e) memperbaiki norma-norma eksisting yang "bermasalah" dalam PP 71/2019 beserta turunannya; dan (f) memberikan akomodasi terhadap PSE yang diselenggarakan secara sektoral untuk pengaturan teknis dalam peraturan perundang-undangan di tiap-tiap bidang.

B. Rekomendasi

Berdasarkan berbagai persoalan yuridis dan empiris yang ditemukan dalam kajian ini, perubahan PP 71/2019 merupakan kebutuhan mendesak yang harus segera diaktualisasikan. Oleh sebab itu, diperlukan pembahasan dan tindak lanjut dari Pemerintah untuk menyusun Rancangan Peraturan Pemerintah tentang Perubahan atas Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Langkah tersebut kian mendesak mengingat dinamika perkembangan dan praktik PSE yang progresif, sehingga membutuhkan upaya hukum yang fleksibel dan cepat dalam mengakomodasi kebutuhan serta permasalahan masyarakat dalam

penyelenggaraan sistem elektronik di Indonesia. Dengan demikian, adanya Naskah Urgensi ini diharapkan dapat mendorong pembahasan dan pengesahan terhadap Rancangan Peraturan Pemerintah tentang Perubahan atas Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

DAFTAR PUSTAKA

A. Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Peraturan Pemerintah Nomor 28 Tahun 2024 tentang Peraturan Pelaksanaan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan.

Peraturan Presiden Nomor 32 Tahun 2024 tentang Tanggung Jawab Perusahaan Platform Digital untuk Mendukung Jurnalisme Berkualitas;

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Peraturan Menteri Komunikasi dan Informatika Nomor 3 Tahun 2021 tentang Standar Kegiatan Usaha dan Standar Produk pada Penyelenggaraan Perizinan Berusaha Berbasis Risiko Sektor Pos, Telekomunikasi, dan Sistem dan Transaksi Elektronik.

Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2025 tentang Penyelenggara Sistem Elektronik Lingkup Publik

Peraturan Menteri Perdagangan Nomor 31 Tahun 2023 tentang Perizinan Berusaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan melalui Sistem Elektronik.

B. Rancangan Peraturan Perundang-Undangan

Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi; dan

C. Produk Hukum Negara Lain atau Organisasi Multinasional

China People Republic's Cybersecurity Law.

China People Republic's Data Security Law.

ChinaPeople Republic's Personal Information Protection Law.

China People Republic Cyberspace Administration of China's Administrative Provisions on Algorithmic Recommendation for Internet Information Services.

European Union General Data Protection Regulation.

European Union Digital Service Act.

Japanese Act on the Protection of Personal Information.

Japanese Basic Act on the Protection of Personal Information.

Japanese Telecommunications Business Act/Act No. 86 of December 25, 1984.

State of California Consumer Privacy Act.

State of Massachusetts General Laws Chapter 93H.

State of New York dan Stop Hacks and Improve Electronic Data Security Act.

State of Texas Business and Commerce Code.

D. Buku

Ali, Z., *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2009).

Basedow, J., Hopt, K. J., *et. al.* (ed.)*, Max Planck Encyclopedia of European Private Law* (Oxford: Oxford University Press, 2012).

Dennis, J., Janecek, K., *et. al., Comparing Privacy Laws: GDPR v. CCPA & CPRA* (Los Angeles: Newmeyer & Dillion, 2022), 10-12.

Fachrurazi (*ed.*), *Fintech dalam Keuangan Islam: Teori dan Praktik* (Jakarta: Publica Indonesia, 2022), 193.

Marzuki, Peter Mahmud, *Penelitian Hukum: Edisi Revisi* (Jakarta: Penerbitan Kencana, 2005).

Muhammad, Abdullah, *Hukum dan Penelitian Hukum* (Bandung: Citra Aditya Bakti, 2004).

The Government of Japan, *Japan Cybersecurity Strategy* (Tokyo: The Government of Japan, 2015).

E. Jurnal/Artikel Ilmiah

Carvalho, J.M., Lima, F.A., Farinha, M., "Introduction to the Digital Services Act, Content Moderation and Consumer Protection," *Revista de Direito e Tecnologia*, vol. 3, no. 1 (2021).

Creemers, R., "China's Emerging Data Protection Framework," *Journal of Cybersecurity*, vol. 8, No. 1 (2022).

Hoecke, M. Van, "Methodology of Comparative Legal Research", *Law and Method,* Vol. 12, No. 1 (2015).

Kostruba, A., Haliantych, M., *et. al,* "Legal Gaps: Concept, Content, Problems of the Role of Legal Doctrine in Overcoming them", *Statute Law Review,* Vol. 44 (Januari 2023).

Lam, H.K.S., Yeung, A.C.L., *et. al.,* "Should Firms Invest in Social Commerce? An Integrative Perspective", *Information and Management,* Vol. 56, No. 8 (Desember 2019), 4-5.

Muliawaty, Lia, Hendryawan, Shofwan, "Peranan *E-Government* dalam Pelayanan Publik (Studi Kasus: Mal Pelayanan Publik Kabupaten Sumedang" *Kebijakan: Jurnal Ilmu Administrasi,* Vol. 11, No. 2 (2020).

Rheinstein, M., "Comparative Law - Its Functions, Methods and Usages", *Arkansas Law Review,* Vol. 22, No. 415 (1968).

Sahib, N. S. M., Idayanti, S., Rahayu, K., "Problematika Aturan Penyelenggara Sistem Elektronik (PSE) di Indonesia", *Pancasakti Law Journal,* Vol 1, No. 1 (Juni 2023).

Zeng, R., Li, X., "On the Illegality and Regulation of Algorithmic Price Discrimination in China's Digital Economy," *Journal of Politics and Law*, vol. 16, no. 4 (2023).

Zhang, C., "China's Privacy Protection Strategy and Its Geopolitical Implications," *Asian Review of Political Economy*, vol. 3, no. 6 (2024).

F. Makalah

Nidhal, M., Indrayadi, S., Budiman, L., *et. al.,* "Makalah Kebijakan Nomor 62: Menelusuri Ulasan *Online* di Indonesia: Dampak pada Platform UGC dan Konsumen".

Tokat, Y., "Are Internet Regulation and Freedom of Speech at odds? How can the Balkanization of the Internet Affect Users' Freedoms on the Internet?", *2021 AJDI Doctoral Student Conference* (Desember 2021).

G. Situs Web

Aliansi Jurnalis Independen, "Serangan terhadap Kebebasan Berekspresi dan Kebebasan Pers Berbahaya Bagi Semua Hak Asasi Manusia Lainnya", AJI Indonesia, https://aji.or.id/informasi/serangan-terhadap-kebebasan-berekspresi-dan-kebebasan-pers-berbahaya-bagi-semua-hak-asasi (diakses 22 November 2025).

Amnesty International, "What the EU's Digital Services Act means for human rights and harmful Big Tech business models", *Amnesty Internasional,* https://www.amnesty.org/en/documents/pol30/5830/2022/en/ (diakses 12 Desember 2025).

Anggraeni, R., "Akuisisi Tokopedia, TikTok Shop Jadi Raksasa e-Commerce Asia Tenggara", *Bisnis.com*, https://ekonomi.bisnis.com/read/20240716/12/1782611/akuisisi-tokopedia-tiktok-shop-jadi-raksasa-e-commerce-asia-tenggara (diakses 10 Desember 2025).

Arai, Y., "History of the Development of Telecommunications Infrastructure in Japan," *Netcom*), https://journals.openedition.org/netcom/4511, https://doi.org/10.4000/netcom.4511 (diakses 23 Februari 2026).

Asih, R. W., "Tak Hanya WhatsApp, Meta AI Juga Bisa Digunakan di Instagram", *Bisnis,* https://teknologi.bisnis.com/read/20241214/84/1824254/tak-hanya-whatsapp-meta-ai-juga-bisa-digunakan-di-instagram (diakses 10 Februari 2026).

Barankova, V., "Innovate UK Global Expert Mission Report: Cyber Security in Japan," *Innovate UK Business Connect,* https://iuk-business-connect.org.uk/wp-content/uploads/2023/09/Japan-Cyber-Security-GEM-Public-FINAL-090823-v2.pdf (diakses 22 Februari 2026).

Bestari, N.P., "Steam Hingga Paypal Diblokir, #BlokirKominfo Menggema", CNBC Indonesia, *https://www.cnbcindonesia.com/tech/20220730111859-37-359795/steam-hingga-paypal-diblokir-blokirkominfo-menggema* (diakses 11 Februari 2026).

Bigg, C., Ge, A., *et. al.,* "CHINA: Enhanced and Clarified Data Compliance Obligations on Handlers of 'Network Data', Covering Personal Information and Important Data, and Operators of Online Platforms from 1 January 2025," *Privacy Matters by DLA Piper*, https://privacymatters.dlapiper.com/2024/10/china-enhanced-and-clarified-data-compliance-obligations-on-handlers-of-network-data-covering-personal-information-and-important-data-and-operators-of-online-platforms-from-1-january-2025/ (diakses 14 Februari 2026).

Bird & Bird, "Data as a Key Digital Asset: China – Data and Evolving Digital Regulation: Algorithm Regulation," *Bird & Bir*d, https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/apac-dra/apac-dsd/data-as-a-key-digital-asset/china/data-and-evolving-digital-regulation-algorithm-regulation (diakses 21 Februari 2026).

Biro Humas Kementerian Komunikasi dan Informatika, "Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data", *Kementerian Komunikasi dan Digital,* https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data/ (diakses 12 Februari 2026).

Biro Komunikasi Kementerian Kesehatan RI, "Pemerintah Terbitkan Aturan Pelaksana UU Kesehatan", Kementerian Kesehatan RI, https://sehatnegeriku.kemkes.go.id/baca/umum/20240730/4346114/pemerintah-terbitkan-aturan-pelaksana-uu-kesehatan/ (diakses 20 Februari 2026).

Briantika, A., Pemblokiran PSE Dinilai Wujud Kegagalan Kominfo Urus Digitalisasi", *Tirto,* https://tirto.id/pemblokiran-pse-dinilai-wujud-kegagalan-kominfo-urus-digitalisasi-guFN (diakses 12 Februari 2026).

Buijs, D., "Article 17 Media Freedom Act & the Digital Services Act: Aligned or Alienated?", *DSA Observatory*, https://dsa-observatory.eu/2022/11/25/article-17-media-freedom-act-the-digital-services-act-aligned-or-alienated/ (diakses 12 Februari 2026).

Cakti, A., "Pakar: PP No. 71 Tahun 2019 beri kejelasan bagi pelaku usaha", *Antara,* https://www.antaranews.com/berita/1145664/pakar-pp-no-71-tahun-2019-beri-kejelasan-bagi-pelaku-usaha (diakses 22 Februari 2026).

CNN Indonesia, "BSSN Sebut Serangan Ransomware Jadi Ancaman Utama di Pilkada 2024", CNN Indonesia, https://www.cnnindonesia.com/nasional/20241107152356-617-1164074/bssn-sebut-serangan-ransomware-jadi-ancaman-utama-di-pilkada-2024 (diakses 23 Februari 2026).

_____, "BSSN Deteksi 44 Juta Aktivitas Malware Hingga Mei 2024", CNN Indonesia, https://www.cnnindonesia.com/teknologi/20240516184354-185-1098626/bssn-deteksi-44-juta-aktivitas-malware-hingga-mei-2024 (diakses 23 Februari 2026).

_____, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual", *CNN Indonesia*, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual (diakses 12 Februari 2026).

_____, "Pengamat Sebut PP PSTE Hanya Regulasi Sementara" *CNN Indonesia,* https://www.cnnindonesia.com/teknologi/20191023071553-185-442020/pengamat-sebut-pp-pste-hanya-regulasi-sementara (diakses 12 Februari 2026).

Captain Compliance, "LGPD Principles," *Captain Compliance,* https://captaincompliance.com/education/lgpd-principles/#h-2-adequacy (diakses 25 Februari 2026).

Clinten, B., Pertiwi, W.K., "Pengguna X Twitter di Indonesia Sudah Bisa Coba Grok, *Chatbot AI* yang Lebih Humoris", *Kompas,* https://tekno.kompas.com/read/2026/05/02/11300077/pengguna-x-twitter-di-indonesia-sudah-bisa-coba-grok-chatbot-ai-yang-lebih (diakses 10 Februari 2026).

_____, Yusuf, O., "Data Ratusan Ribu Nasabah Kredit Plus Diduga Bocor dan Dijual di Internet", *Kompas,* https://tekno.kompas.com/read/2020/08/04/07150007/data-ratusan-ribu-nasabah-kredit-plus-diduga-bocor-dan-dijual-di-internet (diakses 12 Februari 2026).

Cohen, D.L., Savio, T.R., Jiang, J., *et. al*, "Impact of the New China Data Security Law for International Investors and Businesses," *Akin Gump Alerts,* https://www.akingump.com/en/insights/alerts/impact-of-the-new-china-data-security-law-for-businesses-and-international-investors-1 (diakses 15 Februari 2026).

DataGuidance, "The Ultimate Guide to the LGPD," *DataGuidance,* https://www.dataguidance.com/resource/ultimate-guide-lgpd (diakses 25 Februari 2026).

_____, "Japan: Amendments to Telecommunications Business Act Enter into Effect," *Data Guidance,* https://www.dataguidance.com/news/japan-amendments-telecommunications-business-act-enter (diakses 23 Februari 2026).

Direktorat Jenderal Aplikasi dan Informatika Kementerian Komunikasi dan Digital, "Daftar PSE Asing", *Kementerian Komunikasi dan Digital,* https://pse.kominfo.go.id/home/pse-asing (diakses 10 Februari 2026).

_____, “Daftar PSE Domestik”, *Kementerian Komunikasi dan Digital,* https://pse.kominfo.go.id/home/pse-domestik (diakses 10 Februari 2026).

_____, “Jumlah Instansi Publik yang Telah Mendaftar Penyelenggara Sistem Elektronik (PSE)”, *Kementerian Komunikasi dan Digital,* https://data.komdigi.go.id/opendata/dataset/jumlah-instansi-publik-yang-telah-mendaftar-penyelenggara-sistem-elektronik-pse (diakses 10 Februari 2026).

E-Governance Academy, “Indonesia: National Cyber Security Index”, *National Cyber Security Index,* https://ncsi.ega.ee/country/id_2022/ (diakses 23 Februari 2026).

Edge, “Privacy and Personal Data,” *Edge Communications,* https://www.edge.com.vc/en/communication-and-press/privacy-and-personal-data/ (diakses 25 Februari 2026).

Electronic Privacy Information Center, “Data Minimization”, *EPIC.org,* https://epic.org/issues/consumer-privacy/data-minimization/ (Diakses 12 Februari 2026).

European Commission, “Digital Services Act: Questions and Answers,” *European Commission Digital Strategy*, https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers (diakses 11 Februari 2026).

_____, “Digital Services Act Starts Applying to All Online Platforms in the EU,” European Commission Press Corner, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_881 (diakses 12 Februari 2026).

_____, “Questions and Answers on the Digital Services Act”, *European Commission,*

https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_20_2348/QANDA_20_2348_EN.pdf (diakses 12 Februari 2026).

_____, "The Impact of the Digital Services Act on Digital Platforms," *European Commission Digital Strategy*, https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms (diakses 12 Februari 2026).

European Union Agency for Criminal Justice Cooperation, "Digital Services Act – Ensuring a Safe and Accountable Online Environment", *European Union Agency for Criminal Justice Cooperation,*, https://data.europa.eu/doi/10.2812/802073 (diakses 12 Februari 2026).

Farisa, F.C., "Dugaan Kebocoran Data Pemilih Disebut Gerus Kepercayaan Publik ke KPU", *Kompas,* https://nasional.kompas.com/read/2023/11/30/06000061/dugaan-kebocoran-data-pemilih-disebut-gerus-kepercayaan-publik-ke-kpu?page=all. (diakses 12 Februari 2026).

Firdaus, A., "Kasus Kebocoran Data Pribadi di Indonesia: 10 Kejadian Terbesar yang Perlu Diketahui", *Media Indonesia,* https://www.medcom.id/teknologi/news-teknologi/8koPDdWK-kasus-kebocoran-data-pribadi-di-indonesia-10-kejadian-terbesar-yang-perlu-diketahui (diakses 12 Februari 2026).

Fitri, A., "Pernah mengalami kebocoran data, begini cara Bukalapak mengamankan sistemnya", *Kontan,* https://industri.kontan.co.id/news/pernah-mengalami-kebocoran-data-begini-cara-bukalapak-mengamankan-sistemnya (diakses 12 Februari 2026).

Gerst, M., "China's New Cyber Security Law: What It is About and How to Prepare for It", *EU SME Centre*, https://www.eusmecentre.org.cn/publications/chinas-new-cyber-security-law-what-it-is-about-and-how-to-prepare-for-it/ (diakses 14 Februari 2026).

Gobel, T., "RedDoorz Alami Kebocoran Data, Pelanggan Diminta Ganti Password," *Cyberthreat.id*, https://cyberthreat.id/read/8614/RedDoorz-Alami-Kebocoran-Data-Pelanggan-Diminta-Ganti-Password (diakses 12 Februari 2026).

Gong, J., "The Data Security Law of China ('DSL'), Together with the Personal Information Protection Law of China ('PIPL')," *Bird & Bird*, https://www.twobirds.com/en/trending-topics/china-privacy-and-data-protection (diakses 15 Februari 2026).

Harter Secrest & Emery, "California Consumer Privacy Act ('CCPA') and NY SHIELD Act," *Harter Secrest & Emery LLP*, https://hselaw.com/california-consumer-privacy-act-ccpa-and-ny-shield-act/ (diakses 12 Februari 2026).

Hayashi, H., Yukawa, M., Tsuta, D., "Cybersecurity Laws and Regulations: Japan 2025," *ICLG - Cybersecurity Laws and Regulations,* https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan (diakses 24 Februari 2026).

Hollwarth, T., "New Cookie Regulations in Japan – Amendment of Telecommunications Business Act," *EuroCloud News,* https://www.eurocloud.at/news/detail/news/new-cookie-regulations-in-japan-amendment-of-telecommunications-business-act/ (diakses 23 Februari 2026).

Hounslow, D., Nozaki, R., "Japan - Data Protection Overview," *DataGuidance,* https://www.dataguidance.com/notes/japan-data-protection-overview (diakses 22 Februari 2026).

Human Rights Watch, "Peraturan Pelindungan Data Umum Uni Eropa," *Human Rights Watch*, https://www.hrw.org/id/news/2018/06/06/318734 (diakses 11 Februari 2026).

Humas Kementerian Perdagangan RI, "Siaran Pers: PP Nomor 80 Tahun 2019: Pemerintah Lahirkan Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik", Kementerian Perdagangan RI,

https://www.kemendag.go.id/berita/siaran-pers/pp-nomor-80-tahun-2019-pemerintah-lahirkan-peraturan-pemerintah-tentang-perdagangan-melalui-sistem-elektronik (diakses 15 Februari 2026).

Humas Sekretariat Kabinet RI, "Inilah Perpres 32/2024 tentang *Publisher Rights*", Sekretariat Kabinet RI, https://setkab.go.id/inilah-perpres-32-2024-tentang-publisher-rights/ (diakses 20 Februari 2026).

InCountry Staff, "China's Digital Data Sovereignty Laws and Regulations," *InCountry Blog,* https://incountry.com/blog/chinas-digital-data-sovereignty-laws-and-regulations/ (diakses 16 Februari 2026).

Information Commissioner's Office, "Principle (a): Lawfulness, Fairness and Transparency," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/ (diakses 11 Februari 2026).

_____, "Principle (c): Data Minimisation," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/ (diakses 11 Februari 2026).

_____, "Guide to Accountability and Governance," *ICO News*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/ (diakses 11 Februari 2026).

Interesse, G., "China Issues New Regulations on Network Data Security Management, Effective January 1, 2025," *China Briefing,* https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/ (diakses 20 Februari 2026).

Iubenda, "What is LGPD and how do you become compliant?," *IUBENDA,* https://www.iubenda.com/en/help/26706-lgpd-guide (diakses 25 Februari 2026).

Jóźwiak, M., "The Wait Is (Almost) Over! First Risk Assessment and Audit Reports – What Will Be Published, When, and the Way Forward," *DSA Observatory*, https://dsa-observatory.eu/2024/11/22/the-wait-is-almost-over-first-risk-assessment-and-audit-reports-what-will-be-published-when-and-the-way-forward/ (diakses 12 Februari 2026).

Junck, R.D., Klein, B.A., Kumaki, A., *et. al.*, "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies," *Skadden Arps, Slate Meagher & Flom LLP,* https://www.skadden.com/-/media/files/publications/2021/11/chinas_new_data_security_and_personal_information_protection_laws_what_they_mean.pdf?rev=271e4258db3d4a02845addffb7ae4b1c (diakses 14 Februari 2026).

Kawase, T., "Understanding the Chinese Data Security Law: Explaining the Measures Japanese Companies Should Take," *Monolith Law*, https://monolith.law/en/general-corporate/china-data-security-law (diakses 14 Februari 2026).

Kementerian Perdagangan RI, "Menteri Perdagangan Resmi Berlakukan Permendag 31/2023", *Kementerian Perdagangan RI,* https://www.kemendag.go.id/berita/pojok-media/zulhas-resmi-berlakukan-permendag-312023 (diakses 21 Februari 2026).

Kennedy, G., Lai, J. W. J., Wong, J., "PRC Network Data Security Management Regulations," *Mayer Brown Publications,* https://www.mayerbrown.com/en/insights/publications/2024/12/prc-network-data-security-management-regulations (diakses 20 Februari 2026).

Klein, D., "The CPPA and Federal Preemption of State Data Privacy Laws?" *Klein Moynihan Turco LLP*, https://kleinmoynihan.com/the-cppa-and-federal-preemption-of-state-data-privacy-laws/ (diakses 13 Februari 2026).

Kokas, A., "China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges," *China Leadership Monitor* 70, https://www.prcleader.org/post/china-s-2021-data-security-law-grand-data-strategy-with-looming-implementation-challenges (diakses 15 Februari 2026).

Lembaga Studi & Advokasi Masyarakat, "Pendaftaran PSE Lingkup Privat oleh Kominfo Tidak Sesederhana "Tinggal Daftar", Banyak Ancaman Bahaya di Belakangnya", *ELSAM,* https://www.elsam.or.id/siaran-pers/pendaftaran-pse-lingkup-privat-oleh-kominfo-tidak-sesederhana-tinggal-daftar-banyak-ancaman-bahaya-di-belakangnya (diakses 12 Februari 2026).

Li, B., "China's New Cross-Border Data Transfer Regulations: What You Need to Know and Do," *IAPP News,* https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do (diakses 21 Februari 2026).

Luthfiany, D., "Agoda dan Airbnb Cs Terancam Diblokir Pekan Ini, Sandiaga: Kami Ingin Tiap Entitas di RI Ikuti Aturan", *Tempo,* https://www.tempo.co/ekonomi/agoda-dan-airbnb-cs-terancam-diblokir-pekan-ini-sandiaga-kami-ingin-tiap-entitas-di-ri-ikuti-aturan-77298 (diakses 11 Februari 2026).

Mayda, G., Elvaretta, R., "Pembobolan Pusat Data Nasional: Pembelajaran Pemerintah dalam Penguatan Keamanan Perlindungan Data Nasional", *Lembaga Kajian Keilmuan Fakultas Hukum Universitas Indonesia*, https://lk2fhui.law.ui.ac.id/portfolio/pembobolan-pusat-data-nasional-pembelajaran-pemerintah-dalam-penguatan-keamanan-perlindungan-data-nasional/ (diakses 23 Februari 2026).

Ministry of Internal Affairs and Communications, "Report on Telecommunications Policy,"*Ministry of Internal Affairs and Communications*,

https://www.soumu.go.jp/main_content/000979390.pdf (diakses 24 Februari 2026).

Nadarajah, H., Iskandar, A., *et. al.,* "Indonesian Government Under Fire Following String of Cyber Breaches", *Asia Pacific Foundation of Canada,* https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches (diakses 23 Februari 2026).

Newton, C., "Instagram is building a standalone app for shopping", *The Verge,* https://www.theverge.com/2018/9/4/17819766/instagram-shopping-app-e-commerce (diakses 10 Februari 2026).

Ning, S., Wu, H., "Cybersecurity 2022: China Law & Practice and China Trends & Development," *Chambers Global Practice Guides,* https://www.kwm.com/content/dam/kwm/insights/download-publication/china/2023/Chambers%20Cybersecurity%202022.pdf (diakses 15 Februari 2026).

Noorhadi, D. F., "Pro Kontra Aturan PSE", *Informatika Universitas Islam Indonesia*, https://informatics.uii.ac.id/2022/08/15/pro-kontra-aturan-pse/ (diakses 22 Februari 2026).

PriceWaterhouseCoopers, "A Comparison of Cybersecurity Regulations: China," *PwC*, https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html (diakses 14 Februari 2026).

Redaksi Deutsche Welle Indonesia, "Aturan Baru Uni Eropa untuk Bisnis Digital Mulai Berlaku," *DW.com*, https://www.dw.com/id/aturan-baru-uni-eropa-untuk-bisnis-digital-mulai-berlaku/a-66628099 (diakses 12 Februari 2026).

Rizky, V., "ELSAM Nilai PP PSTE Hanya Berlaku Sementara", *Jogja Aja,* https://jogjaaja.com/read/elsam-nilai-pp-pste-hanya-berlaku-sementara (diakses 23 Februar 2026).

Sandy, O. P., "PP 71/2019 Dinilai Tak Pro Industri Data Center Lokal", *Cyberthreat Indonesia,* https://cyberthreat.id/read/3628/PP-712019-Dinilai-Tak-Pro-Industri-Data-Center-Lokal (diakses 22 Februari 2026).

Satria, I.R.T.B., "Hidup Sungguh Amat Sederhana, tapi Dibuat Ribet Kominfo dan PSE", *Mojok,* https://mojok.co/esai/hidup-sungguh-amat-sederhana-tapi-dibuat-ribet-kominfo-dan-pse/ (diakses 12 Februari 2026).

Sayuri, U., "Japan: Basic Act on Cybersecurity Amended," *Global Legal Monitor, Library of Congress*, https://www.loc.gov/item/global-legal-monitor/2018-12-26/japan-basic-act-on-cybersecurity-amended/ (diakses 24 Februari 2026).

Simmons, D., "CPPA Board Opposes American Data Privacy and Protection Act," *Alston & Bird LLP Privacy Blog,* https://www.alstonprivacy.com/cppa-board-opposes-american-data-privacy-and-protection-act/ (diakses 13 Februari 2026).

Silfia, I., "Pemerintah himpun pajak Rp29,97 triliun dari sektor ekonomi digital", *Antara,* https://www.antaranews.com/berita/4463121/pemerintah-himpun-pajak-rp2997-triliun-dari-sektor-ekonomi-digital (diakses 10 Februari 2026).

Smith, R., "MLPS 2.0: China's Enhanced Data Security Multi-Level Protection Scheme and Related Enforcement Updates," *Reed Smith*, https://www.reedsmith.com/en/perspectives/2019/10/mlps-20-chinas-enhanced-data-security-multi-level-protection (diakses 14 Februari 2026).

Sun, O., "Cross-Border Data Transfer Mechanism in China and Its Compliance," *California Lawyers Association*, https://calawyers.org/business-law/cross-border-data-transfer-mechanism-in-china-and-its-compliance/ (diakses 15 Februari 2026).

Takase, K., Tatsuno, D., "Japan Enacts Amendments to the Act on the Protection of Personal Information," *Baker McKenzie InsightPlus,* https://insightplus.bakermckenzie.com/bm/investigations-compliance-

ethics/japan-enacts-amendments-to-the-act-on-the-protection-of-personal-information (diakses 23 Februari 2026).

The Federal Trade Commission, "2023 Privacy and Data Security Update", *US FTC,* https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf (diakses 12 Februari 2026).

Thomson Reuters, "Understanding the California Consumer Privacy Act (CCPA)," *Reuters*, https://legal.thomsonreuters.com/en/insights/articles/understanding-california-consumer-privacy-act (diakses 13 Februari 2026).

Urban, J., Hennessy, J., "State Data Breach Notification Laws," *Foley & Lardner LLP*, https://www.foley.com/insights/publications/2024/11/state-data-breach-notification-laws/ (diakses 12 Februari 2026).

Yuniarto, T., "Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya", *Kompas,* https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya (diakses 23 Februari 2026).

Zhang, Z., "A Close Reading of China's New Cybersecurity Review Measures, in Effect Feb 15, 2022," *China Briefing,* https://www.china-briefing.com/news/a-close-reading-of-chinas-new-cybersecurity-review-measures-in-effect-february-15-2022/ (diakses 15 Februari 2026).

Zuraya, N., "Facebook Luncurkan Fitur Belanja Shops di Indonesia", *Republika,* https://ekonomi.republika.co.id/berita/qfyu7y383/facebook-luncurkan-fitur-belanja-shops-di-indonesia (diakses 10 Februari 2026).

