Tantangan Mewujudkan Pelindungan Data Pribadi dalam Tata Kelola Data di Sektor Kesehatan dan Pendidikan

Penulis
Fuji Aotari Wahyu Anggreini
Lamia Putri Damayanti
Indri D. Saptaningrum

Penyunting
Debora Irene Christine

KERTAS KEBIJAKAN
YAYASAN TIFA | MEI 2022

DAFTAR ISI

Tantangan Mewujudkan Pelindungan Data Pribadi dalam Tata Kelola Data di Sektor Kesehatan dan Pendidikan

1. Pendahuluan

Pandemi Covid-19 yang mulai memasuki Indonesia sejak tahun awal tahun 2020 membawa perubahan mendasar terhadap penyelenggaraan layanan publik dan intensitas penggunaan teknologi informasi dan komunikasi digital dalam penyediaan layanan publik. Dua sektor penting yang segera merasakan dampak dari pandemi adalah sektor kesehatan dan pendidikan. Pandemi telah memaksa pemerintah untuk merumuskan respons cepat dan tepat dalam menekan laju penyebaran virus dan jumlah infeksi. Kebutuhan adanya respons yang cepat dalam pengendalian pandemi juga mendorong intensitas penggunaan aplikasi digital untuk pelacakan *(tracking)* dan penelusuran kontak erat *(tracing)*, seperti aplikasi PeduliLindungi, dan percepatan realisasi penyediaan data terpadu untuk meningkatkan efisiensi penyediaan layanan publik yang tepat guna.[1]

Kebijakan pengendalian pandemi melalui penerapan pembatasan mobilitas sosial mendorong perubahan pola dan model pembelajaran melalui pembelajaran daring. Perubahan model pembelajaran ini mensyaratkan dukungan ketersediaan dan tata kelola data yang memadai. Dalam realisasinya, penyelenggaraan pembelajaran daring menghadapi banyak kendala. Merujuk pada data Badan Pusat Statistik (BPS) di tahun 2020, sebanyak 3% (45 juta siswa) kehilangan kesempatan untuk melanjutkan kegiatan belajar di sekolah.[2] Sementara itu, infrastruktur telekomunikasi yang belum memadai menjadi masalah utama bagi penyediaan akses internet yang merata. Secara khusus, intensitas penggunaan teknologi dalam layanan publik di sektor kesehatan dan pendidikan penting untuk dikaji lebih jauh karena melibatkan pemrosesan data pribadi warga negara sebagai penerima layanan. Upaya menegakkan jaminan perlindungan data pribadi melalui pengembangan tata kelola pemrosesan data yang dilandasi prinsip perlindungan hak asasi manusia (HAM) telah menjadi fokus perhatian dan kerja Tifa, serta banyak organisasi masyarakat sipil lainnya.

Berangkat dari rumusan masalah di atas, Yayasan Tifa bersama Centre for Innovation Policy and Governance (CIPG) dengan dukungan Luminate melaksanakan kajian dan advokasi kebijakan untuk menelusuri lebih dalam kompleksitas tata kelola data digital pada pelayanan publik di sektor kesehatan dan pendidikan selama pandemi Covid-19. Dalam penyusunan kertas kebijakan ini, pengumpulan data dilakukan pada November 2021 hingga April 2022 melalui penggalian data empiris, yaitu melakukan serangkaian wawancara dengan berbagai pemangku kepentingan tata kelola data sektor kesehatan dan pendidikan. Pengumpulan data dilaksanakan di tingkat nasional (Indonesia), provinsi (Jawa Barat) dan kota/kabupaten (Pontianak) dengan mewawancarai perwakilan dari Kementerian Kesehatan (Kemenkes), Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi (Kemendikbud Ristek), Dinas Kesehatan, Dinas Pendidikan, dan Dinas Komunikasi dan Informasi (Diskominfo). Selain wawancara, studi pustaka juga dilakukan untuk memperkaya hasil temuan.

Secara khusus, kertas kebijakan ini bertujuan melengkapi penelitian sebelumnya dengan mendalami implementasi keamanan data dan pelindungan data pribadi

1 Sebagai contoh, salah satu isu penting yang mempengaruhi kinerja layanan kesehatan adalah keterlambatan pemberian tunjangan tenaga kesehatan, yang salah satunya bersumber dari akurasi dan ketersediaan data. Lihat ICW, Percepatan Penyaluran Insentif dan Santunan Tenaga Kerja Kesehatan dalam Penanganan Covid19, Februari 2021. Diakses di https://antikorupsi.org/sites/default/files/dokumen/Policy%20Brief%20Insentif%20Nakes_FINAL_compressed.pdf.

2 Lihat Nadia Fairuza Azzahra, Mengkaji Hambatan Pembelajaran Jarak Jauh di Indonesia di Masa Pandemi Covid-19: Seri Ringkasan Kebijakan No. 2, CIPS, Mei 2020. Diakses di https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_beb2bbe622c241409452fe6803a410f0.pdf

serta mengeksplorasi hubungan antara penyelenggaraan kebijakan desentralisasi struktur administrasi pemerintahan dengan pelaksanaan tata kelola data di sektor kesehatan dan pendidikan. Pada bagian awal kertas kebijakan ini, penulis memaparkan relevansi instrumen internasional HAM bagi tata kelola data. Selanjutnya, penulis menjabarkan kerangka normatif dan prinsip-prinsip umum tata kelola data yang diatur dalam berbagai ketentuan perundang-undangan di Indonesia. Berdasarkan uraian normatif ini, bagian keempat mendiskusikan temuan-temuan pengelolaan data pada sektor kesehatan dan pendidikan. Pada bagian akhir kertas kebijakan, penulis mengemukakan sejumlah rekomendasi.

2. Prinsip-Prinsip Internasional Tata Kelola Data

Data elektronik/digital (dalam jumlah yang besar) memiliki peran vital dalam pengembangan berbagai layanan baik publik maupun privat yang bersifat komersial. Perkembangan teknologi informasi dan komunikasi mendorong peningkatan produksi data dan volume transmisi data setiap detiknya. Setidaknya sebanyak 500 jam konten diunggah pengguna melalui *platform* Youtube dan sebanyak 197,6 juta *email* ditransmisikan melalui internet setiap menitnya.[3] Selain peningkatan eksponensial dalam aspek volume data dan jumlah pengguna data, perkembangan penggunaan teknologi digital dalam pelayanan publik juga berimplikasi pada pengumpulan data yang bersifat sensitif seperti data pribadi yang terkait dengan rekam jejak kesehatan. Selain itu, digitalisasi layanan publik juga berimplikasi pada peningkatan kebutuhan dan pertukaran akses data antarlembaga pemerintah dan antara lembaga pemerintah dan pihak swasta penyedia layanan telekomunikasi. Hal ini menimbulkan risiko bagi keamanan data pribadi dan privasi. Dengan demikian, tata kelola data menjadi satu prasyarat penting dalam memastikan terselenggaranya layanan publik yang akuntabel.

Meskipun memiliki peran vital, sampai saat ini tidak terdapat satu rujukan baku atas pengertian tata kelola data. Tata kelola data lebih umum diasosiasikan dengan kebutuhan praktis organisasi untuk mengatur akses dan keamanan data. Menurut Data Governance Institute, tata kelola data dirumuskan sebagai:

> "... suatu sistem pengambilan keputusan mengenai hak dan tanggung jawab atas proses-proses yang terkait dengan informasi, yang dilakukan berdasarkan model yang telah disepakati, yang menggambarkan siapa yang dapat mengambil tindakan apa, dengan informasi yang mana dan kapan, serta dalam situasi-situasi seperti apa, dengan mempergunakan metode-metode tertentu."[4]

Berdasarkan rumusan tersebut, tata kelola data pada dasarnya merupakan suatu fungsi manajemen pengelolaan informasi. Pengelolaan ini berfungsi untuk menjamin kualitas, integritas, keamanan dan kegunaan data dalam satu siklus hidupnya dari sejak pertama kali data dikumpulkan sampai saat di mana data harus dimusnahkan.[5]

Dalam konteks penerapan tata kelola untuk penyelenggaraan layanan publik oleh badan-badan pemerintah, Organisasi Kerjasama Ekonomi dan Pembangunan (OECD) mengembangkan sepuluh prinsip praktik terbaik pengelolaan data untuk sektor publik sebagai panduan bagi pemerintah berbagai negara untuk merumuskan kebijakan dan tata kelola data di sektor publik. Kesepuluh prinsip tersebut adalah:[6]

- Integritas dalam pengelolaan data
- Tahu dan mematuhi peraturan terkait di seluruh pemerintahan untuk akses, *sharing* dan penggunaan data yang dapat dipercaya
- Memasukkan pertimbangan etis mengenai data ke dalam proses pembuatan keputusan pemerintah, organisasi dan sektor publik

3 Lori Lewis, Infographic: What Happens In An Internet Minute 2021, 13 April 2021. Diakses di https://www.allaccess.com/merg Seae/archive/32972/infographic-what-happens-in-an-internet-minute

4 Data Governance Institute, Defining Data Governance. Diakses di https://datagovernance.com/defining-data-governance/

5 Evren Eryurek, et.al., Data Governance, The Definitive Guide: People, Processes, and Tools to Operationalise Data Trustworthiness, O'Reilly, 2021, hal. 8-10.

6 OECD, Good Practice Principles for Data Ethics in the Public Sector, March 2021, hal.7-11. Diakses di https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf

- Memantau dan mempertahankan pengawasan atas input data, terutama data yang dipergunakan untuk pengembangan dan pelatihan sistem kecerdasan buatan (*artificial intelligence*), dan mengadopsi pendekatan berbasis risiko dalam penerapan otomatisasi keputusan.
- Spesifik mengenai tujuan penggunaan data, terutama dalam hal data pribadi
- Menentukan batasan untuk akses data, *sharing* dan penggunaan data
- Bersikap jelas, inklusif dan terbuka
- Mempublikasikan data terbuka dan sumber kode terbuka
- Memperluas kontrol individu dan kolektif terhadap data mereka
- Akuntabel dan proaktif dalam mengelola risiko

Karena ketiadaan satu ketentuan baku untuk mengatur tata kelola data, pengembangan sistem tata kelola data sangat tergantung pada konteks lokal masing-masing negara, tingkat kebutuhan penggunaan dan akses data, serta kemampuan masing-masing negara dalam menyediakan infrastruktur tata kelola data yang memadai. Hal ini membuat penyelenggaraan tata kelola data umumnya mengacu pada prinsip-prinsip umum seperti yang dikembangkan oleh OECD tersebut di atas.

Selain itu, pelaksanaan tata kelola data untuk sektor publik juga dipengaruhi oleh perkembangan hukum dan standar hak asasi manusia, khususnya yang terkait dengan pelindungan privasi dan data pribadi. Bahkan dalam perkembangan mutakhir, elemen hak asasi manusia telah sepenuhnya terintegrasi dalam standar dan prinsip tata kelola data, serta menjadi pertimbangan penting dalam pengembangan tata kelola data di sektor publik.[7]

Data pribadi merupakan bagian tak terpisahkan dari hak atas privasi yang diatur dalam Pasal 12 Deklarasi Hak Asasi Manusia (DUHAM) dan Pasal 17 Kovenan Hak Sipil dan Politik (ICCPR). Berdasarkan pengaturan tersebut, setiap negara pihak dari kovenan wajib mengatur melalui suatu undang-undang yang jelas, mengenai perekaman, pemrosesan, penggunaan dan transmisi secara otomatis terhadap data pribadi, serta melindungi mereka yang memperoleh dampak dari penyalahgunaan data pribadi, baik oleh institusi negara maupun swasta.[8] Merujuk data United Nations Conference on Trade and Development (UNCTAD), sampai saat ini setidaknya sebanyak 194 negara telah memiliki ketentuan hukum baik yang berbentuk undang-undang maupun ketentuan hukum lainnya untuk melindungi data dan privasi.[9]

Standar perlindungan data pribadi tercantum dalam berbagai dokumen yang dikembangkan oleh badan-badan Persatuan Bangsa-Bangsa (PBB) dan beberapa institusi internasional seperti OECD (OECD privacy Guidelines, 1980)[10]. Selain itu terdapat pula prinsip-prinsip privasi yang disepakati secara internasional maupun di Uni Eropa seperti Convention 108+ dan General Data Protection Regulation (GDPR),[11] yang menjadi salah satu kerangka kerja perlindungan atas data pribadi yang mendasari perubahan kerangka perlindungan data pribadi secara global. Di tingkat Asia Tenggara, Association of Southeast Asian Nations (ASEAN) juga telah mengadopsi rujukan kerangka perlindungan data pribadi yang tertuang dalam ASEAN Framework on Personal Data Protection di tahun 2016, sebagai bagian mewujudkan integrasi ekonomi kawasan melalui ekonomi digital yang aman, berkelanjutan dan transformatif.[12]

Kemunculan berbagai kerangka rujukan tersebut telah mengembangkan standar-standar global yang berlaku dalam pemrosesan data pribadi. OECD merumuskan delapan prinsip umum yang berlaku sebagai standar minimum dalam pemrosesan data pribadi; EU-GDPR merumuskan sembilan prinsip umum pemrosesan data pribadi; dan ASEAN Framework on Personal Data Protection memuat

7 Sebagai contoh, lihat OECD (2013), Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges, OECD Health Policy Studies, OECD Publishing. Diakses di http://dx.doi.org/10.1787/9789264193505-en

8 A/HRC/17/27, Par. 58.

9 UNCTAD, Data Protection and Privacy Legislation Worldwide. Diakses di https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

10 OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013. Diakses di https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

11 Official Journal of European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Diakses di https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

12 ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Framework on Personal Data Protection. Diakses di https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

tujuh prinsip umum dalam pemrosesan data pribadi termasuk pemrosesan data yang melibatkan arus perpindahan data antar negara. Dari berbagai rujukan tersebut, dapat dirumuskan prinsip-prinsip umum yang berlaku dalam pemrosesan data pribadi:

a. **Prinsip keabsahan hukum (*lawfulness*)**
   Pemrosesan data pribadi memerlukan dasar hukum dan harus dilakukan secara sah menurut hukum. Syarat sah pemrosesan data memiliki beberapa elemen, di antaranya kewajiban adanya persetujuan (*consent*) dan pengetahuan dari subyek data mengenai pemrosesan data pribadinya. Selain itu, pemrosesan data pribadi juga menuntut adanya kepentingan yang sah (*legitimate interest*) yang dapat mencakup kepentingan sebagaimana diatur dalam undang-undang atau peraturan hukum lainnya.
b. **Prinsip keadilan *(fairness*)**
   Pemrosesan data pribadi dilakukan secara adil dalam kaitannya dengan subjek data. Dalam prinsip yang dikembangkan oleh OECD, aspek prinsip keadilan menjadi bagian dari prinsip pembatasan pengumpulan data. Pembatasan dilakukan dengan memberikan dua ketentuan utama, yakni keabsahan dan adil, yang mencakup kewajiban untuk memastikan subjek data mengetahui atau memberikan persetujuan atas pengumpulan data pribadi tersebut.
c. **Prinsip transparansi (*transparency*)**
   Prinsip transparansi dalam pemrosesan data pribadi mengharuskan subjek data mengerti dan memahami alasan, tujuan, dan proses pengolahan data. Selain itu subjek data harus dibekali dengan informasi yang cukup agar dapat memperoleh pemenuhan hak-hak terkait dengan penggunaan data pribadinya.
d. **Prinsip tujuan yang terbatas**
   Pemrosesan data pribadi harus dilakukan dengan memenuhi suatu tujuan tertentu yang spesifik dan sah secara hukum. Oleh karena itu, apabila telah dikumpulkan, data pribadi tidak dapat dipergunakan untuk tujuan-tujuan lain selain dari yang telah diumumkan pada saat pengumpulannya. Meski demikian, dalam konteks ini pemrosesan data pribadi lebih lanjut untuk kepentingan publik (*public interest*) dapat dibenarkan sebagai bagian dari realisasi pemrosesan dengan tujuan terbatas ini.
e. **Prinsip minimalisasi pengumpulan data (*minimization*)**
   Pemrosesan data pribadi sedapat mungkin hanya dilakukan sebatas untuk mencapai tujuan yang telah ditetapkan dan tidak dapat dipergunakan melampaui tujuan tersebut. Dengan demikian, prinsip ini menegaskan pemrosesan data pribadi harus dibatasi seminimal mungkin sejauh diperlukan.
f. **Prinsip ketepatan**
   Prinsip ketepatan terkait implementasi pemrosesan data yang dilakukan terutama dalam konteks membuat profil, di mana informasi yang dikumpulkan haruslah bersifat spesifik. Dalam prinsip-prinsip yang dikembangkan OECD, prinsip ini tercakup dalam prinsip kualitas data, yang mensyaratkan ketepatan dan relevansi informasi terhadap tujuan pengumpulannya.
g. **Prinsip pembatasan penyimpanan**
   Prinsip pembatasan waktu penyimpanan data pribadi memiliki pengertian bahwa pemrosesan data pribadi hanya dapat disimpan dalam batas waktu tertentu sejauh diperlukan untuk mencapai tujuan pemrosesannya. Dengan demikian, prinsip ini dapat mencakup kewajiban penghapusan data yang telah dikumpulkan apabila tujuan telah tercapai.
h. **Prinsip integritas dan konfidensialitas**
   Prinsip integritas dan konfidensialitas berkaitan dengan aspek keamanan dalam proses pengolahan data sampai data pribadi yang dikumpulkan dan diolah tetap terjaga keutuhan dan keamanannya. Dalam konteks ini, institusi pemroses data memiliki kewajiban untuk mengambil langkah dan prosedur teknis yang diperlukan untuk menjaga keamanan.
i. **Prinsip akuntabilitas**
   Prinsip akuntabilitas merujuk pada kewajiban untuk menjamin bahwa proses pengumpulan data pribadi wajib dilakukan sesuai dengan seluruh prinsip-prinsip yang berlaku serta dapat dipertanggungjawabkan.

Kesembilan prinsip tersebut telah secara luas diterapkan dalam berbagai ketentuan perundang-undangan di berbagai negara, maupun di tingkat regional dan internasional. Lebih jauh, sebagian besar dari prinsip-prinsip tersebut juga telah menjadi dasar perumusan standar tata kelola data pribadi, dan perlindungan atas hak privasi.

Dalam konteks pandemi, urgensi penerapan prinsip-prinsip ini tercermin antara lain dalam catatan Sekretaris Jenderal PBB pada tahun 2021, sebagai respons atas tindakan negara-negara dalam penanganan pandemi Covid-19 yang kerap mengabaikan perlindungan terhadap hak privasi demi kepentingan

mendesak pencegahan virus Corona.[13] Dalam seruannya, badan PBB menegaskan pentingnya respons terhadap pandemi yang tetap mengedepankan prinsip perlindungan hak atas privasi, termasuk dalam penerapan teknologi untuk kepentingan *contact tracing*, maupun dalam penyediaan layanan publik lainnya.

Selain itu, penerapan prinsip-prinsip umum pemrosesan data pribadi ini juga mengenal pemilahan data pribadi dalam dua kategori umum, yakni data pribadi dan data sensitif. Sebagai contoh, meskipun dalam panduan umum mengenai data pribadi OECD tidak secara eksplisit merumuskan definisi data sensitif, panduan OECD mengakui adanya variasi dan cakupan pengertian yang bervariasi terhadap data yang bersifat sensitif. Oleh karena itu, panduan tersebut menegaskan perlunya tiap negara melakukan penyesuaian dalam penerapan panduan dengan mempertimbangkan sensitivitas data dan karakteristik pemrosesan data yang bervariasi dari satu negara ke negara lainnya.

Lebih lanjut, pengertian dan klasifikasi data sensitif secara tegas diatur dalam EU-GDPR, yang merumuskan cakupan pengertian data sensitif yaitu mencakup:

- data genetik;[14]
- data biometrik yang diproses sebagai sarana untuk mengidentifikasi seseorang sebagai manusia;[15]
- data kesehatan;[16]
- data terkait orientasi seksual maupun kehidupan seksual seseorang;[17]
- mengungkapkan akar ras dan etnis, pandangan politik, agama dan kepercayaan filosofinya;[18]
- keanggotaan pada serikat pekerja.[19]

Perumusan kategori data sensitif selain meningkatkan perlindungan subjek data dari kemungkinan praktik diskriminasi yang terkait dengan akses terhadap layanan publik, juga berimplikasi pada kewajiban untuk meningkatkan keamanan dan integritas sistem pemrosesan data pribadi. Klasifikasi data ini juga telah secara luas diadopsi baik secara eksplisit maupun implisit dalam berbagai peraturan hukum mengenai data pribadi termasuk di Indonesia sebagaimana diuraikan lebih lanjut dalam pemaparan di bawah ini.

3. Kerangka Hukum Tata Kelola Data di Indonesia

Terdapat beberapa kerangka normatif yang mendasari penyelenggaraan tata kelola data di sektor publik. Salah satunya adalah Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang meletakkan dasar migrasi sistem pemerintahan ke ranah digital. Terdapat pula Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia yang meletakkan aturan mengenai standar data, klasifikasi data, pemakaian data, dan mekanisme bagi data. Selanjutnya, ada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang diubah melalui Undang-Undang Nomor 19 Tahun 2016.

Kebutuhan terhadap tata kelola data di sektor publik berhubungan dengan program pemerintah untuk mewujudkan tata kelola pemerintahan berbasis elektronik seperti dimandatkan dalam Perpres 95/2018. Perubahan tata kelola pemerintahan ini ditujukan untuk meningkatkan efisiensi layanan publik. Perpres SPBE meletakkan kerangka dasar penyelenggaraan tata kelola data bagi lembaga-lembaga pemerintah, dari aspek infrastruktur, aplikasi, proses bisnis, dan keamanan data yang terintegrasi. Lebih jauh, arsitektur tata kelola data yang dikembangkan berdasarkan Perpres SPBE mengharuskan integrasi proses bisnis tata kelola data dari pusat sampai ke daerah. Ketentuan ini meletakkan prinsip-prinsip tata kelola data, termasuk keamanan, efisiensi, interoperabilitas, dan akuntabilitas sistem elektronik.[20]

Pengembangan sistem pemerintahan berbasis elektronik ini kemudian diperkuat dengan penetapan Perpres 39/2019. Apabila Perpres SPBE mengatur arsitektur teknis sistem informasi dan mandat dan fungsi institusi, Perpres Satu Data meletakkan

13 Right to privacy, note by the Secretary General, 23 July 2021, A/76/220.
14 Regulation (EU) 2016/679 of the European Parliament and of the Council, Pasal 4 (13).
15 Ibid., Pasal 4 (14).
16 Ibid., Pasal 4 (15).
17 Ibid., Pasal 9 (1).
18 Ibid., Pasal 9 (1) .
19 Ibid., Recitals (71) & (72).
20 Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Pasal 2.

kerangka normatif untuk klasifikasi data di sektor publik, prosedur akses, berbagi, dan penggunaan data untuk sektor publik. Perpres Satu Data merumuskan tujuan pengelolaan data dengan memberikan kerangka acuan pelaksanaan dan pedoman bagi lembaga-lembaga negara, baik di tingkat pusat dan daerah, serta mendorong transparansi pengelolaan data dan mewujudkan ketersediaan data yang akurat dan dapat dipertanggungjawabkan.[21] Implikasi dari berlakunya peraturan-peraturan tersebut ialah pemerintah harus menggunakan satu basis data nasional, seperti data kependudukan yang menerapkan prinsip interoperabilitas data di berbagai institusi yang memiliki kewenangan.

Pilar ketiga dalam penyelenggaraan tata kelola data di sektor publik juga bermuara pada perlindungan hak atas privasi, yang menjadi dasar pengembangan kerangka hukum perlindungan pemrosesan data pribadi. Namun hingga saat ini, payung hukum yang secara spesifik mengatur tentang pelindungan data pribadi di Indonesia belum disahkan. Apabila merujuk pada peraturan yang berlaku, UU ITE telah mengatur perlindungan hak atas privasi, khususnya Pasal 26 ayat (1) yang merumuskan hak pribadi mencakup hak untuk menikmati kehidupan pribadi, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai, dan hak untuk mengawasi akses informasi terhadap kehidupan seseorang. Dengan demikian, pasal tersebut bisa menjadi acuan utama dalam berbagai aturan turunan yang berkaitan dengan data pribadi.

Selain UU ITE, peraturan lainnya yang juga beririsan dengan data pribadi adalah Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP). Di mana pada Pasal 17 huruf h memberikan landasan tambahan mengenai informasi yang termasuk rahasia pribadi yang harus dijaga, terdiri dari:

- riwayat dan kondisi anggota keluarga;
- riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang;
- kondisi keuangan, aset, pendapatan, dan rekening bank seseorang;
- hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang;
- catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.

Di samping peraturan-peraturan tersebut di atas, setidaknya terdapat 32 peraturan setingkat undang-undang yang mengatur dan merumuskan tentang data pribadi secara berbeda-beda, sehingga menimbulkan adanya tumpang tindih aturan mengenai data pribadi.[22] Di tingkat peraturan teknis, pengaturan pokok mengenai prinsip tata kelola data pribadi juga tersebar dalam berbagai aturan pelaksanaan undang-undang yang berbeda. Kajian ini hanya merujuk pada dua aturan teknis utama yang mengatur mengenai pelindungan data pribadi, yakni Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

Meski demikian, kedua peraturan tersebut juga tidak merumuskan subjek pengaturan secara konsisten. Sebagai ilustrasi, pengertian data pribadi pada Permenkominfo 2/2016 dirumuskan secara berbeda dengan PP 71/2019. Definisi data pribadi dalam Permenkominfo lebih menekankan karakteristiknya sebagai suatu informasi yang bersifat khusus yang mencerminkan elemen-elemen umum dalam pengertian data pribadi seperti dijumpai dalam berbagai rujukan ketentuan internasional.[23] Sementara perumusan dalam PP 71/2019 lebih menonjolkan sifat teknis data pribadi dalam kaitannya dengan sistem elektronik.[24]

Permenkominfo 20/2016 lahir sebagai respons terhadap kekosongan pengaturan yang spesifik terkait perlindungan data pribadi. Berdasarkan ketentuan ini, perlindungan data pribadi mencakup sepuluh bentuk tindakan terhadap informasi yang bersifat pribadi, meliputi:[25]

21 Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia, Pasal 2.

22 ELSAM, Undang-Undang Pelindungan Data Pribadi Penting Segera Diwujudkan, Siaran Pers, 7 Maret 2018. Diakses di https://elsam.or.id/uu-perlindungan-data-pribadi-penting-segera-diwujudkan/

23 Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Pasal 1 angka 1.

24 PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), Pasal 1 angka 29.

25 Permenkominfo No. 20 Tahun 2016, Pasal 3.

Permenkominfo 20/2016	PP 71/2019
Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.	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 nonelektronik

Tabel 3.1. Definisi data pribadi dalam Permenkominfo 20/2016 dan PP 71/2019

- perolehan dan pengumpulan;
- pengolahan dan penganalisisan;
- penyimpanan;
- penampilan, pengumuman, pengiriman, penyebarluasan atau pembukaan akses;
- pemusnahan.

Bentuk-bentuk tindakan tersebut mencerminkan keseluruhan proses pengolahan informasi, dimulai dari perolehan informasi sampai ke pemusnahan informasi tersebut. Cakupan ini diperluas dengan penambahan unsur perbaikan dan pembaharuan data pada PP 71/2019.[26]

3.1. Asas-Asas Umum Pemrosesan Data Pribadi

Lebih lanjut, Permenkominfo 20/2016 juga telah mengadopsi sebagian prinsip-prinsip umum pemrosesan data pribadi sebagaimana diuraikan pada bagian sebelumnya. Permenkominfo 20/2016 memuat sepuluh asas perlindungan data pribadi dalam pemrosesan data oleh penyelenggara sistem elektronik baik bersifat privat maupun publik, yaitu:

a. Asas penghormatan terhadap data pribadi sebagai privasi.
b. Asas kerahasian, yaitu data pribadi bersifat rahasia sesuai persetujuan atau ketentuan peraturan perundang-undangan.[27] Di samping itu, pemilik data pribadi juga memiliki hak untuk menyatakan data pribadinya bersifat rahasia.
c. Asas persetujuan di mana pemrosesan data pribadi mewajibkan adanya persetujuan dari subjek data.[28] Penerapan asas persetujuan ini juga berlaku dalam tindakan yang melibatkan pembukaan kerahasian data pribadi. Artinya, kecuali pemilik data memberikan persetujuan pengungkapan kerahasiaan data pribadinya, pemrosesan data pribadi wajib menjaga kerahasiaan data tersebut.
d. Asas relevansi tujuan yang mensyaratkan tindakan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan data pribadi harus relevan dengan tujuannya.[29] Dalam konteks ini, pengolahan dan analisis data pribadi wajib dinyatakan secara jelas sejak saat pengumpulannya dan wajib memperoleh persetujuan dari subjek data.[30] Namun, kewajiban memperoleh persetujuan ini dikecualikan untuk data pribadi yang diperoleh dari informasi yang telah diumumkan secara terbuka untuk pelayanan publik.[31]
e. Asas kelaikan sistem elektronik yaitu pemrosesan data pribadi mensyaratkan adanya kelaikan sistem elektronik yang digunakan. Pada praktiknya, kelaikan sistem elektronik ini ditunjukkan dengan pemenuhan kewajiban memperoleh sertifikasi elektronik sebagaimana diatur dalam UU ITE.
f. Asas itikad baik di mana pemroses data pribadi memiliki kewajiban untuk segera memberitahukan secara tertulis kepada pemilik data pribadi atas setiap kegagalan perlindungan data pribadi.
g. Asas ketersediaan aturan internal pengelolaan perlindungan data pribadi yang mengharuskan pemroses data (atau penyelenggara sistem elek-

26 PP No. 71 Tahun 2019, Pasal 14 ayat (2).

27 Konsep persetujuan dalam asas ini memiliki pengertian yang sama dengan konsep consent yang dikenal baik dalam prinsip umum pemrosesan data dalam GDPR maupun dalam panduan OECD.

28 PP No. 71 Tahun 2019, Pasal 14 (3).

29 Ibid., Pasal 14.

30 Permenkominfo No. 20 Tahun 2016, Pasal 12 ayat (1) dan (2).

31 Ibid., Pasal 13.

tronik) untuk memiliki aturan internal mengenai perlindungan data pribadi sebagai sarana mencegah terjadinya kegagalan melakukan perlindungan terhadap data yang dikelolanya. Upaya pencegahan ini juga mencakup aspek-aspek non-teknis seperti peningkatan kesadaran sumber daya manusia melalui pelatihan yang relevan.[32]

h. Asas tanggung jawab yang diartikan sebagai kemauan pemroses data untuk bertanggung jawab atas data pribadi yang berada dalam penguasaannya.
i. Asas kemudahan akses dan koreksi yang terpenuhi ketika pemilik data pribadi memiliki kemudahan akses dan kemudahan melakukan koreksi terhadap data pribadinya.
j. Asas keutuhan, akurasi, dan keabsahan serta kemutakhiran data pribadi yang mencakup kewajiban dan prasyarat verifikasi. Terdapat dua jenis verifikasi yang diatur dalam Permenkominfo 20/2016, yakni verifikasi langsung apabila data pribadi tersebut diperoleh dan dikumpulkan secara langsung. Verifikasi langsung terjadi di mana data pribadi yang dikumpulkan tersebut diverifikasi secara langsung ke pemilik data pribadi. Sementara verifikasi tidak langsung dengan melakukan verifikasi berdasar hasil olahan dari berbagai sumber.[33]

3.2. Prasyarat Pemrosesan Data Pribadi

Pemrosesan data pribadi untuk berbagai tujuan yang disepakati oleh pemilik data pribadi harus memenuhi beberapa persyaratan agar dapat dinyatakan sah secara hukum. PP 71/2019 memberikan tujuh prasyarat yang harus dipenuhi sebelum pemrosesan data pribadi dapat dilakukan. Sebagian prasyarat ini sebenarnya juga merupakan aspek yang ditemui dalam prinsip-prinsip umum pemrosesan data seperti diuraikan pada bagian sebelumnya. Adapun prasyarat tersebut yakni:[34]

- Adanya persetujuan yang sah dari pemilik data pribadi untuk satu atau beberapa tujuan tertentu.
- Didasarkan pada tujuan pemenuhan perjanjian, dalam hal pemilik data pribadi adalah salah satu pihak dalam perjanjian.
- Didasarkan pada tujuan pemenuhan kewajiban hukum pengendali data pribadi seperti diatur dalam ketentuan perundang-undangan.
- Bertujuan untuk memenuhi perlindungan kepentingan yang sah (*vital interest*) dari pemilik data.
- Sebagai bagian dari pelaksanaan kewenangan pengendali data pribadi.
- Sebagai pemenuhan kewajiban pengendali data pribadi dalam pelayanan publik untuk kepentingan umum.
- Sebagai pemenuhan kepentingan yang sah lainnya dari pengendali data pribadi atau pemilik data pribadi.

Pemenuhan prasyarat ini melengkapi beberapa ketentuan lain yang terkait kewajiban untuk menjamin keamanan data dalam pemrosesan data pribadi.

3.3. Kewajiban Penjaminan Keamanan Data Pribadi

PP 71/2019 juga mengatur beberapa hal penting yang terkait dengan syarat-syarat keamanan pada pemrosesan data pribadi. Prasyarat keamanan ini meliputi keamanan terkait dengan aspek teknis sistem elektronik dan sistem informasinya, serta yang terkait dengan prosedur pemrosesan informasinya. Dalam konteks ini, keamanan sistem elektronik mencakup prasyarat jaminan keamanan perangkat keras yang dipergunakan, maupun perangkat lunak yang mendukung pemrosesan data. Untuk memenuhi prasyarat ini, perangkat keras yang dipergunakan wajib dilengkapi dengan sertifikasi keamanan.[35]

Beberapa kewajiban yang terkait dengan perlindungan keamanan informasi mencakup:

a. Menyediakan perjanjian keamanan informasi atas jasa layanan teknologi informasi yang dipergunakan.[36]
b. Kewajiban melakukan enkripsi atas data pribadi yang ada dalam penguasaannya.
c. Pembatasan masa waktu penyimpanan (retensi) selamanya 5 tahun kecuali apabila di atur secara berbeda oleh peraturan perundang-undangan.
d. Pemberitahuan tertulis kepada pemilik data pribadi bilamana terjadi kegagalan dalam pelindungan terhadap data pribadi yang dikelolanya.
e. Adanya kebijakan tata kelola dan prosedur audit sistem informasi secara reguler serta penerapan manajemen risiko.

32 Ibid., Pasal 5 ayat (4).
33 Ibid., Pasal 10 ayat (2).
34 PP No. 71 Tahun 2019, Pasal 14 ayat (3) dan (4).
35 Ibid.,, Pasal 7 ayat (1a) dan Pasal 8.
36 Ibid., Pasal 11.

Selain itu, terdapat beberapa prasyarat yang dikhususkan bagi pemroses data yang merupakan institusi publik, seperti kewajiban memiliki pusat data dan penyimpanan data di Indonesia. Apabila penyelenggaraan pemrosesan data melibatkan pihak ketiga (entitas privat), pengelola data wajib melakukan klasifikasi data berdasarkan tingkat risiko yang ditimbulkan. Dari ketentuan tersebut, terlihat bahwa aspek keamanan, baik yang terkait dengan sistem elektronik, perangkat keras, maupun informasi yang dikelola merupakan faktor penting untuk mewujudkan tata kelola data yang dapat melindungi data pribadi.

PP 71/2019 mengikutsertakan beberapa prinsip pelindungan data pribadi yang telah dijelaskan di atas. Pasal 14, misalnya, mensyaratkan pemrosesan data yang harus dilakukan secara tepat dan akurat, adanya mekanisme retensi dalam setiap pemrosesan data, hingga adanya kewajiban untuk mendapatkan persetujuan subjek data. Contoh-contoh di atas merefleksikan telah dimuatnya prinsip transparansi, tujuan yang terbatas, minimalisasi pengumpulan data, ketepatan, pembatasan penyimpanan, serta integritas dan konfidensialitas. Selain Pasal 14, Pasal 15 sampai dengan Pasal 18 juga memuat prinsip-prinsip di atas, termasuk pentingnya kewajiban untuk menghapus data-data yang tidak lagi relevan dengan tujuan pemrosesan data.

4. Tantangan dalam Penerapan Prinsip-Prinsip Tata Kelola Data di Sektor Kesehatan dan Pendidikan

Kerangka normatif yang mengatur mengenai arsitektur teknis, proses bisnis, dan standar tata kelola data untuk sektor publik seperti diuraikan dalam bagian terdahulu memberikan rujukan penting bagi kementerian dan lembaga negara yang terkait dalam implementasinya di sektor kesehatan dan pendidikan. Meskipun demikian, kerangka normatif yang tersedia tidak selalu dapat direalisasikan sepenuhnya, baik karena faktor internal birokrasi, kapasitas institusional, maupun hal-hal teknis. Dalam bagian berikut ini, dipaparkan hasil studi kasus mengenai pengelolaan data di sektor kesehatan dan pendidikan. Studi kasus yang pertama dilakukan untuk melihat implementasi kebijakan penyediaan data dalam mendukung pengendalian pandemi, melalui (1) penyediaan data layanan fasilitas kesehatan, (2) penelusuran individu dan komunitas terdampak pandemi melalui pengembangan aplikasi, dan (3) integrasi data pandemi dengan data kependudukan untuk mendukung layanan kesehatan. Sementara itu, studi kedua melihat implementasi prinsip dan ketentuan normatif mengenai tata kelola data yang dibahas pada bagian sebelumnya di sektor pendidikan, khususnya kebijakan yang dikembangkan sebagai respon atas pandemi, seperti (4) pengembangan dukungan kuota data untuk pembelajaran daring dan (5) penyediaan informasi pendidik dan peserta didik serta situasi pembelajaran melalui pengembangan sistem data pokok pendidikan (dapodik).

Temuan utama dari studi kasus ini mengungkapkan tiga masalah kunci yang menghambat perwujudan tata kelola data yang efisien, tepat guna, dan dapat dipertanggungjawabkan untuk mendukung respon pemerintah terhadap pandemi Covid-19. Ketiga masalah kunci tersebut adalah, *pertama,* adanya ketidaksesuaian aturan hukum di tingkat pusat dan daerah dalam mendukung ekosistem tata kelola data yang baik, termasuk persoalan perbedaan definisi data pribadi antara Permenkominfo 20/2016 dengan PP 71/2019; *kedua,* kurang memadainya infrastruktur sistem informasi, yang antara lain menimbulkan tantangan bagi keamanan dan interoperabilitas data; *ketiga,* kurang memadainya kapasitas kelembagaan pelaksana tata kelola data. Kapasitas kelembagaan ini mencakup kecukupan mandat institusional, anggaran, dan kapasitas teknis personel Kementerian/Lembaga terkait. Ketiga problem tersebut akan didiskusikan secara lengkap dalam bagian berikut ini.

4.1. Tata Kelola Data di Sektor Kesehatan

Pandemi Covid-19 mendorong transformasi digital yang masif guna mendukung pencegahan penularan Covid-19. Karakteristik Covid-19 yang menyebar dengan sangat cepat mengharuskan pemerintah dan berbagai lapisan masyarakat untuk menyiasati penanggulangan serta pencegahan pandemi. Upaya yang dilakukan selama beberapa tahun terakhir adalah dengan pemberlakukan pembatasan sosial serta 3T (*testing, tracing, treatment)* seperti yang diamanatkan oleh Organisasi Kesehatan Dunia (WHO). Perubahan ini berdampak signifikan bagi aktivitas dan interaksi sosial anggota masyarakat, misalnya, kewajiban penggunaan aplikasi PeduliLindungi setiap memasuki fasilitas umum.

Kajian di sektor kesehatan ini menemukan tiga kendala utama yang menghambat implementasi tiga pilar kerangka normatif yang diuraikan pada bagian tiga dalam tata kelola data kesehatan, khususnya yang dilakukan sebagai respon terhadap pandemi Covid-19. *Pertama*, kendala yang terkait dengan regulasi, khususnya adanya perbedaan antara aturan normatif dalam Perpres dan Undang-undang dengan aturan pelaksana baik di tingkat kementerian maupun di tingkat daerah. *Kedua*, kesiapan dan kapasitas lembaga pelaksana tata kelola data, termasuk kemampuan menyediakan infrastruktur teknis dan infrastruktur fasilitas layanan kesehatan maupun sumber daya manusia yang belum mumpuni. *Ketiga*, belum terintegrasinya sistem informasi yang andal, aman dan terpercaya sehingga mengakibatkan kualitas data yang tidak optimal.

Kesenjangan antara peraturan-peraturan tata kelola data di sektor kesehatan

Secara umum, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan telah mengatur mengenai pembangunan dan pelaksanaan sistem informasi di sektor kesehatan untuk mewujudkan penyelenggaraan layanan yang efektif. Lebih lanjut, aturan pelaksanaan UU ini telah mengatur mengenai standar, prosedur, dan tahapan pengembangan infrastruktur teknis yang diperlukan dalam pengembangan tata kelola data. Aspek-aspek penting dalam implementasi sistem informasi ini diatur melalui peraturan-peraturan turunan sebagai berikut:

a. Peraturan Pemerintah Nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan (SIK) merupakan turunan dari UU 36/2009. Dalam hal ini, SIK yang dimaksud adalah seperangkat tatanan yang meliputi data, informasi, indikator, prosedur, perangkat, teknologi, dan sumber daya manusia yang saling berkaitan dan dikelola secara terpadu untuk mengarahkan tindakan atau keputusan yang berguna dalam mendukung pembangunan kesehatan. PP ini juga mengatur mekanisme pengumpulan, prinsip pengolahan, penyimpanan, dan pengamanan data serta informasi kesehatan yang termaktub dalam Pasal 17 hingga 24. Pengumpulan data dilakukan dengan beberapa cara seperti pengumpulan data rutin yang dilakukan oleh tenaga kesehatan, rekam medik, dan surveilans. Pengolahan data meliputi pemrosesan, analisis, dan penyajian. Penyimpanan data yang dimaksud dalam PP ini adalah menyimpan data kesehatan dengan aman agar tidak rusak dan tetap utuh sehingga dapat digunakan sebagaimana mestinya. PP ini juga mengatur mekanisme retensi yang mensyaratkan penyimpanan data selama 10-25 tahun saja. Sementara itu, pengamanan dan jaminan kerahasiaan data diatur dalam Pasal 23. Dalam hal ini, tanggung jawab yang dibebankan pada pengelola sistem informasi kesehatan hanya spesifik pada keamanan data yang merujuk pada penyimpanan, pemeliharaan, pencadangan data, serta pencegahan kerusakan sistem. Secara keseluruhan, PP ini banyak menyebutkan prosedur penyimpanan dan pengamanan data tetapi tidak membahas prinsip-prinsip pelindungan data pribadi.
b. Peraturan Menteri Kesehatan Nomor 97 Tahun 2015 tentang Peta Jalan Sistem Informasi Kesehatan 2015-2019 mengatur pentingnya penguatan sistem informasi kesehatan untuk menghasilkan data dan informasi kesehatan yang andal dan mudah diakses. Permenkes ini mengatur peta jalan penyelenggaraan SIK selama 2015-2019.
c. Peraturan Pemerintah Nomor 46 Tahun 2017 tentang Strategi e-Kesehatan Nasional menjelaskan tentang upaya peningkatan kualitas, aksesibilitas, dan kesinambungan pelayanan kesehatan. PP tersebut menjelaskan bahwa untuk meningkatkan ketersediaan dan kualitas data dan informasi kesehatan, diperlukan penerapan teknologi informasi dan komunikasi di bidang kesehatan yang disebut e-kesehatan. Peraturan ini meregulasi pelaksanaan sistem informasi dan implementasi layanan kesehatan berbasis elektronik. Permenkes ini mengatur secara rinci mengenai aspek-aspek teknis untuk mewujudkan infrastruktur tata kelola informasi, namun tidak mengatur prinsip-prinsip pelindungan data dan batasan-batasan dalam pengelolaan data. Berdasarkan penelitian yang dilakukan oleh Centre for Innovation Policy and Governance (CIPG) e-kesehatan juga membutuhkan regulasi teknis dan SOP yang rigid dalam pelaksanaannya.[37]

Berdasarkan peraturan-peraturan yang telah dijelaskan di atas, ketentuan hukum normatif sebenarnya telah memberikan landasan konseptual

37 Esti, K., Novianda, A. H., Suhanda, K. (2022). Menata Kelola Data demi Pelayanan Publik: Studi Kasus Tata Kelola Data Sektor Kesehatan dan Pendidikan di Indonesia selama Pandemi Covid-19. Jakarta: Centre for Innovation Policy and Governance dan Yayasan Tifa.

dan mengatur aspek-aspek teknis penyelenggaraan tata kelola data di sektor publik. Namun, pelindungan data pribadi tidak dibahas secara spesifik. Adapun aspek pelindungan data pribadi lebih banyak dikemas dalam prinsip-prinsip keamanan data. Tabel 4.1. merangkum integrasi prinsip-prinsip pelindungan data pribadi dalam peraturan-peraturan di atas.

Peraturan Perundang-Undangan	Pasal terkait Pelindungan Data Pribadi / Keterangan	Prinsip Pelindungan Data Pribadi
PP 46/2014	Pasal 15-20	Prinsip tujuan yang terbatas Prinsip minimalisasi pengumpulan data (*minimization*)
	Pasal 21	Prinsip pembatasan penyimpanan
	Pasal 23	Prinsip integritas dan konfidensialitas
Permenkes 97/2015	Menjelaskan peta jalan sistem informasi kesehatan serta peluang dan tantangan untuk mewujudkannya	Prinsip integritas dan konfidensialitas, terutama dalam kaitannya dengan keamanan data
PP 46/2017	Memuat strategi e-kesehatan untuk upaya peningkatan kualitas layanan kesehatan yang berkaitan dengan pengembangan teknologi informasi dan komunikasi.	Prinsip integritas dan konfidensialitas, terutama dalam kaitannya dengan keamanan data

Tabel 4.1. Prinsip-prinsip pelindungan data pribadi dalam peraturan-peraturan yang menjadi landasan penyelenggaraan tata kelola data di sektor kesehatan

Minimnya pengintegrasian pilar pelindungan data pribadi dalam peraturan tata kelola data juga terjadi di peraturan tingkat daerah. Berdasarkan penggalian informasi di dua daerah di level kabupaten/kota dan provinsi, yakni Kota Pontianak dan Provinsi Jawa Barat, peraturan daerah yang ditetapkan untuk mengatur tata kelola data di sektor kesehatan hanya menyinggung tentang keamanan data, tetapi tidak secara komprehensif mengintegrasikan aspek pelindungan data pribadi.

Provinsi Jawa Barat memiliki peraturan terkait tata kelola data yang terdapat dalam Peraturan Daerah Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik, dan Persandian, serta Peraturan Gubernur Nomor 13 Tahun 2020 tentang Rencana Induk Sistem Pemerintahan Berbasis Eletronik Pemerintah Daerah Provinsi Jawa Barat Tahun 2019-2023. Perda 4/2021 telah memuat aspek-aspek penting terkait tata kelola data, baik prinsip bagi pakai hingga mekanisme partisipasi publik. Namun, peraturan ini belum memuat penyeragaman standarisasi data dan mekanisme pelindungan data pribadi secara detail.

Sementara itu, Pergub 13/2020 juga belum mengatur secara rinci mengenai pelindungan data pribadi. Sama halnya dengan Provinsi Jawa Barat, Kota Pontianak juga memiliki aturan terkait mengenai tata kelola data, yakni Peraturan Walikota Nomor 46 Tahun 2021 tentang Satu Data Kota Pontianak. Peraturan ini telah memuat prinsip bagi pakai dan mengatur secara jelas mengenai penyelenggaraan Satu Data. Namun, aturan ini belum membahas secara spesifik mengenai pelindungan data pribadi dan penyelenggaraan Satu Data di saat krisis seperti pandemi.

Kapasitas kelembagaan: keterbatasan infrastruktur layanan kesehatan, kesiapan birokrasi, dan kapasitas personel

Dalam praktiknya, baik layanan kesehatan maupun tata kelola data kesehatan sulit dilaksanakan secara berkualitas secara bersamaan, khususnya pada saat tingkat penularan wabah meningkat secara cepat. Dari segi infrastruktur dan layanan kesehatan, Indonesia masih di bawah standar internasional dalam pemenuhan hak kesehatan. Berdasarkan data Kementerian Kesehatan, rasio tempat tidur rumah sakit di Indonesia sebesar 1,17 per 1.000 penduduk

pada tahun 2018. Artinya, Indonesia hanya memiliki 1 tempat tidur rumah sakit per 1.000 penduduknya. Angka ini sangat jauh jika dibandingkan dengan Korea Selatan yang memiliki kurang lebih 11 tempat tidur rumah sakit per 1.000 penduduk.[38]

Selain itu, rasio jumlah tempat tidur di tiap wilayah juga tidak sama. Hal ini disebabkan oleh ketimpangan infrastruktur dan akses terhadap ketersediaan rumah sakit di masing-masing daerah. DKI Jakarta menjadi wilayah yang memiliki tempat tidur rumah sakit terbanyak di Indonesia. Saat ini, DKI Jakarta mampu menyediakan 2 tempat tidur rumah sakit per 1.000 penduduknya. Sementara rasio dokter di Indonesia untuk 1000 warga hanya sampai 0,67%, sedangkan rata-rata kebutuhan dokter di Asia mencapai 1,2%. Keterbatasan tenaga kesehatan, terutama dokter, menjadi salah satu penyebab tidak tertanganinya pandemi selama pecahnya wabah pada gelombang kedua. Di Indonesia bagian timur, seperti Maluku dan Papua, 50% fasilitas layanan kesehatan bahkan tidak memiliki dokter yang bertugas.[39]

Studi kasus di Jawa Barat menunjukkan adanya hubungan antara ketersediaan infrastruktur layanan kesehatan, jumlah sumber daya manusia (SDM), dan proses integrasi data antara daerah dan pusat. Ketika wabah terjadi, tenaga kesehatan memprioritaskan penyediaan layanan bagi masyarakat dibanding pengelolaan sistem informasi dan data. Proses integrasi data di daerah dan pusat dapat dilakukan dengan lebih optimal ketika situasi pandemi mulai stabil.[40]

Keterbatasan wewenang pemerintah daerah juga menyulitkan implementasi tata kelola data. Kewenangan penuh tata kelola data berada di Kementerian Kesehatan sementara pemerintah daerah menunggu arahan dari pemerintah pusat. Dinas Kesehatan di tingkat provinsi, misalnya, memiliki pengetahuan yang terbatas mengenai infrastruktur aplikasi tata kelola data kesehatan yang dikembangkan oleh pemerintah pusat, seperti *National All Record* (NAR), *Silacak*, dan *P-Care,* dan kapasitas terbatas dalam proses pengelolaannya. Selain itu, proses memasukkan data ke sistem kesehatan dilakukan oleh pemerintah kabupaten/kota sementara Dinkes Provinsi berperan sebagai regulator pengawas, fasilitator, dan pembina. Implementasi tata kelola data di tingkat kabupaten/kota sendiri menunggu arahan dari provinsi.

Dari hasil pertemuan bilateral dengan Dinas Kesehatan Provinsi Jawa Barat, beberapa pihak mengakui bahwa hal tersebut menjadi salah satu penyebab belum optimalnya penyelenggaraan tata kelola data sektor kesehatan.[41] Selain terbatasnya kewenangan pemerintah daerah, pengelolaan infrastruktur data yang tersentralisasi di pemerintah pusat juga dapat memperlambat kinerja petugas tata kelola data kesehatan di tingkat daerah. Dalam situasi kegagalan fungsi *server*[42] yang dapat menyebabkan basis data pusat tidak bisa diakses, misalnya, petugas harus mengisi data secara manual[43] ke aplikasi Kesehatan. Hal ini menjadi beban kerja ganda bagi petugas.

Dalam penyelenggaraan tata kelola data, ketersediaan infrastruktur serta kapasitas institusional di masing-masing daerah dapat menjadi tolak ukur kesiapan birokrasi. Jawa Barat merupakan contoh provinsi yang gesit dalam tata kelola data. Saat kasus COVID-19 pertama kali ditemukan, Pemprov Jawa Barat langsung membangun sistem informasi dan komunikasi berbasis *website* untuk menyebarluaskan informasi terkait COVID-19. Inisiatif ini kemudian berkembang menjadi aplikasi Pusat Informasi dan Koordinasi COVID-19 Jawa Barat (Pikobar) yang hingga saat ini digunakan untuk mendukung penanggulangan pandemi.

Aplikasi Pikobar dibangun dengan *host* dan *server* yang dikelola sendiri oleh pemerintah daerah. Dalam pelaksanaannya, kerja sama dengan pihak ketiga hanya ditujukan untuk mendukung integrasi antar-aplikasi kesehatan untuk mempermudah penanggulangan pandemi, misalnya, dengan mengintegrasikan Pikobar dengan layanan kesehatan daring Halodoc. Keberada-

38 Databoks, Ini Rasion Tempat Tidur Rumah Sakit 34 Provinsi di Indonesia, 30 Maret 2020. Diakses di https://databoks.katadata.co.id/datapublish/2020/03/30/ini-rasio-tempat-tidur-rumah-sakit-34-provinsi-di-indonesia, pada 2 April 2022.

39 Medcom.id, Indonesia Masih Kekurangan SDM Kesehatan, 19 Desember 2021. Diakses di https://www.medcom.id/nasional/politik/5b2GlxnkIndonesia-masih-kekurangan-sdm-kesehatan, pada 2 April 2022.

40 Hasil Pertemuan Bilateral dengan Dinas Kesehatan dan Dinas Informasi dan Komunikasi Provinsi Jawa Barat pada Maret 2021.

41 Ibid.

42 Server atau dalam bahasa Indonesia biasa disebut peladen merupakan suatu sistem komputer yang memiliki layanan khusus berupa penyimpanan data. Data yang disimpan melalui server berupa informasi dan beragam jenis dokumen yang kompleks.

43 Hasil Pertemuan Bilateral dengan Dinas Informasi dan Komunikasi Provinsi Jawa Barat pada Maret 2022.

an Pikobar mengurangi tumpang tindih data dan mendukung percepatan penyediaan layanan kesehatan seperti isolasi mandiri dan pengiriman obat serta vitamin kepada warga.

Meski demikian, implementasi tata kelola data kesehatan di Jawa Barat menghadapi kendala terkait integrasi data aplikasi kesehatan dengan aplikasi yang dikelola pemerintah pusat. Sebagai aplikasi yang lebih dulu dibangun dan digunakan, diperlukan penyesuaian dengan aplikasi-aplikasi yang dikembangkan oleh pemerintah pusat dengan yang digunakan di daerah. Karena adanya keharusan menggunakan aplikasi yang dikelola pemerintah pusat, Pikobar saat ini dikembangkan sebagai pusat data *(hub)*. Jika ada data kesehatan yang memang dibutuhkan dengan cepat, Dinkes Provinsi tidak perlu meminta data dari pemerintah pusat, tetapi langsung mengambil dari Pikobar. Dalam proses pengembangan Pikobar sebagai pusat data, terdapat kebutuhan untuk mengintegrasikan data yang disimpan di Pikobar dengan aplikasi yang dikembangkan oleh pemerintah pusat. Proses integrasi masih belum dapat dilakukan secara utuh karena Kemenkes menangani seluruh proses integrasi data dan aplikasi dari berbagai daerah.

Kesiapan infrastruktur digital yang memengaruhi kualitas akses internet, ketersediaan sumber daya manusia yang kompetensinya sesuai, serta tata kelola data kesehatan yang terpadu, merupakan faktor-faktor kontekstual yang menunjukkan bahwa Indonesia memiliki banyak tugas untuk memenuhi tata kelola data yang baik. Dalam hal ini, kesenjangan digital juga perlu menjadi perhatian pemerintah. Sebab, meski aplikasi membantu layanan publik, tetapi tidak semua pihak mampu mengakses aplikasi tersebut. Sehingga, dalam beberapa hal, aplikasi justru mengeksklusi masyarakat marjinal.

Selain itu, adanya perbedaan definisi dan konsep mengenai tata kelola data di tingkat daerah dan pusat juga menyebabkan adanya perbedaan pemahaman mengenai peran dan tanggung jawab tenaga kesehatan. Perbedaan ini misalnya saja, berdampak pada tidak sinkronnya data antara pusat dan daerah karena perbedaan standarisasi. Selain perbedaan pemahaman di level internal sektor kesehatan, Dinas Kesehatan juga menemui adanya perbedaan pemahaman data dari pihak eksternal. Sebagai contoh, pihak eksternal seperti TNI dan Polri kerap meminta data dari Dinas Kesehatan. Tetapi, data yang diminta tidak memiliki standar data yang telah dikelola Dinkes. Sehingga, Dinkes perlu menyesuaikan data sesuai dengan permintaan data dari pihak yang eksternal yang tentu saja mengakibatkan beban ganda.[44]

E-kesehatan Indonesia dinilai belum memenuhi beberapa aspek, seperti investasi yang belum memadai di infrastruktur dan SDM TIK, sistem informasi yang tidak seragam dan belum sepenuhnya terintegrasi, serta standarisasi kualitas, terminologi, keamanan, interoperabilitas, dan protokol pertukaran data. Hal ini sangat penting untuk segera dilakukan karena implementasi e-kesehatan lintas sektor.

Kendala integrasi data dan interoperabilitas sistem

Dalam penanganan pandemi, pemerintah pusat menjadi pihak yang memiliki otoritas dalam penyelenggaraan tata kelola data. Data adalah kewenangan dari Kementerian Kesehatan, sedangkan Dinas Kesehatan (Dinkes) di level provinsi maupun daerah tidak bisa terlibat lebih dalam terkait tata kelola data.[45] Mekanisme input dan penyelenggaraan tata kelola data oleh provinsi dan daerah menunggu arahan dari pusat. Namun, dalam pelaksanaannya, tata kelola data yang terpusat justru menghambat pemerintah daerah dalam mengambil keputusan. Selain itu, data di tingkat pusat dan tingkat daerah juga tidak sinkron. Hal ini disebabkan oleh beberapa hal, di antaranya:

a. Perbedaan definisi "data" dalam Perda dan Perpres Satu Data. Dalam Perda Jabar 4/2021, misalnya data didefinisikan sebagai informasi yang berupa angka tentang karakteristik (ciri-ciri khusus) suatu populasi. Sedangkan dalam Perpres 39/2019, data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar,peta, tanda, isyarat, tulisan, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi. Perbedaan pengertian dan definisi dapat menghambat implementasi tata kelola data karena berpotensi menimbulkan pemahaman yang

44 Hasil Pertemuan Bilateral dengan Dinas Kesehatan Kota Pontianak pada bulan November 2021.

45 Hasil Pertemuan Bilateral dengan Dinas Kesehatan Provinsi Jawa Barat pada November 2021.

berbeda-beda terutama terkait dengan standarisasi data dan metadata, Berdasarkan prinsip Satu Data Indonesia, data yang dihasilkan oleh produsen data harus memenuhi standar data, memiliki metadata, menggunakan kode referensi atau data induk, dan memenuhi kaidah interoperabilitas data yang mana dapat dilakukan jika konsep data yang dipahami oleh masing-masing pihak, baik daerah maupun pusat, bersumber dari konsep/peraturan yang sama.

b. Terlalu banyaknya aplikasi kesehatan yang digunakan di Indonesia. Saat ini, pemerintah pusat mencatat setidaknya ada 60 aplikasi kesehatan yang dalam Sistem Informasi Kesehatan Indonesia, baik yang dikembangkan oleh pemerintah pusat maupun daerah. Hal ini tentu menyulitkan proses integrasi data.
c. Ketiadaan standar interoperabilitas. Standar interoperabilitas merupakan rangkaian spesifikasi yang perlu dipenuhi agar berbagai sistem informasi dapat berkomunikasi satu sama lain. Dalam konteks pengembangan aplikasi kesehatan, standar interoperabilitas menjadi rujukan yang menetapkan bentuk, sintak, struktur, penyajian, dan semantik data elektronik agar dapat dibagitukarkan dari satu aplikasi dengan aplikasi lainnya. Jika diimplementasikan dengan baik, interoperabilitas sistem informasi kesehatan dapat mendukung terselenggaranya pelayanan publik yang lebih efisien. Ketiadaan standar interoperabilitas di Indonesia membuat implementasi prinsip keterpaduan dan interoperabilitas dalam tata kelola data sektor kesehatan masih terbatas, sehingga data yang masuk di sistem kurang bisa dimanfaatkan sepenuhnya.

Proses integrasi antara pusat dan daerah saat ini masih berjalan cukup lambat dikarenakan perlunya sinkronisasi antar aplikasi. Namun, dalam kasus yang ditemukan di Jawa Barat, proses integrasi bisa dipercepat dengan adanya komunikasi tradisional antara pemerintah provinsi dan pusat. Komunikasi tradisional yang dimaksud di sini adalah proses komunikasi yang tidak berada dalam infrastruktur mekanisme aplikasi itu sendiri. Jadi, pemerintah daerah yang tidak memiliki akses langsung ke pusat tidak dapat mempercepat proses integrasi jika memang benar-benar dibutuhkan.[46] Sementara itu, pusat tidak hanya mengurus satu provinsi saja tetapi juga semua provinsi di Indonesia. Dalam implementasinya, kualitas data masih belum sinkron, simpang siur, dan tidak akurat. Perlu penguatan standar kualitas, terminologi, keamanan, interoperabilitas, dan protokol pertukaran data.

Keamanan dan privasi data

Keamanan data menjadi salah satu kunci utama dalam setiap mekanisme tata kelola data. Namun, dalam pelaksanaannya, tidak ada jaminan hukum yang jelas untuk perlindungan keamanan data karena ketiadaan Undang-Undang Pelindungan Data Pribadi (PDP) di Indonesia. Peraturan mengenai tata kelola data dalam PP 71/2019 memang telah menjamin kerahasiaan data pribadi. Dalam Pasal 14, penyelenggaraan sistem elektronik harus memuat prinsip-prinsip pelindungan data pribadi. PP tersebut juga telah menyinggung tanggung jawab pengendali data. Namun aturan tersebut belum menjelaskan secara spesifik mengenai mekanisme serta hak dan tanggung jawab pemilik, pemroses data, dan walidata.

Meski PP 71/2019 telah memuat prinsip pelindungan data pribadi, namun aturan ini tidak diturunkan dalam PP 46/2014 dan Permenkes 46/2017. Hal ini menyulitkan implementasi tata kelola data dalam sektor kesehatan karena setiap pemrosesan memuat data-data sensitif yang harus dilindungi. Pemerintah pun memahami kebutuhan akan regulasi yang secara spesifik mengatur pelindungan data pribadi untuk mempermudah penyelenggaraan layanan publik.

Selain karena tidak adanya payung hukum yang spesifik, pelindungan data pribadi di sektor kesehatan sulit dilakukan karena pemahaman pemangku kepentingan yang masih minim tentang data pribadi dan indikator keamanan data.[47] Beban kerja ganda tenaga kesehatan yang juga harus melaksanakan fungsi administratif tata kelola data di samping tugas utama mereka melakukan upaya kesehatan adalah faktor lainnya yang menghambat implementasi tata kelola data kesehatan yang baik. Pasal 58(c) Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan menegaskan bahwa tenaga kesehatan berkewajiban menjaga kerahasiaan kesehatan peneri-

46 Hasil Pertemuan Bilateral dengan Jabar Digital Service (JDS) Provinsi Jawa Barat pada Maret 2022.

47 Hasil Pertemuan Bilateral dengan Dinas Kesehatan Kota Pontianak pada November 2021.

ma pelayanan kesehatan. Selain itu, beragamnya aplikasi yang digunakan dalam Sistem Informasi Kesehatan membuat tenaga kesehatan harus mampu mengoperasikan aplikasi-aplikasi tersebut sesuai dengan situasi kesehatan yang mereka hadapi.

Tidak hanya itu, hak dan tanggung jawab pengolah data juga belum dijelaskan secara rinci dalam peraturan pelindungan data pribadi. Dalam konteks pandemi yang sedang berlangsung, pengelolaan data dituntut harus cepat dan mampu mengolah volume data yang masif. Hal ini berpotensi besar menyebabkan keluputan (*human error*) ketika data dimasukkan ke sistem.[48] Dalam hal ini, diperlukan penguatan kapasitas terkait data pribadi dan petugas khusus yang bertugas untuk memastikan keamanan data. Penguatan kapasitas dapat dilakukan dengan pelatihan berkelanjutan secara bertahap seperti: (1) pelatihan literasi digital dalam pengoperasian teknologi digital, (2) pelatihan keamanan digital, (3) literasi data, (4) pemahaman mengenai keamanan siber di sektor kesehatan, serta (5) pemahaman mengenai pelindungan data pribadi (data umum, data pribadi, dan data sensitif).

Selain keamanan data, konsep privasi juga perlu digalakkan. Keamanan dan privasi data adalah dua hal yang berbeda namun keduanya saling beririsan terutama ketika berkaitan dengan aplikasi digital, baik aplikasi kesehatan yang dikembangkan oleh pemerintah pusat dan daerah, maupun pihak swasta. Penggunaan aplikasi seperti PeduliLindungi menjadi salah satu kewajiban bagi publik jika ingin berpergian maupun mendatangi sarana umum. Keputusan Menteri Komunikasi dan Informatika Nomor 171 Tahun 2020 tentang Penetapan Aplikasi Pedulilindungi Dalam Rangka Pelaksanaan Surveilans Kesehatan Penanganan Corona Virus Disease 2019 (Covid-19). Saat ini pemerintah menggunakan aplikasi PeduliLindungi untuk pelacakan kontak dan informasi mengenai vaksin. Meskipun terintegrasi dengan 80 aplikasi lainnya, termasuk Tokopedia, Gojek, Traveloka, Grab, dan Dana, PeduliLindungi tidak membagi data dengan aplikasi-aplikasi tersebut tanpa seizin pemilik data. Pengguna PeduliLindungi memiliki kuasa penuh untuk menentukan izin akses pihak ketiga terhadap data pribadi yang tersimpan di aplikasi.

Mengingat bahwa data pribadi yang tersimpan di aplikasi PeduliLindungi sangat sensitif, dibutuhkan mekanisme keamanan data pribadi dan mitigasi kebocoran data. Penelitian CIPG menunjukkan bahwa belum ada jaminan keamanan data pada aplikasi PeduliLindungi yang menggunakan platform Google. Meski penelitian tersebut juga menekankan bahwa belum ada temuan faktual kebocoran data aplikasi PeduliLindungi, rekam jejak kebocoran data dari sistem BPJS dan e-HAC mengindikasikan lemahnya keamanan sistem informasi kesehatan Indonesia. Dengan demikian, keamanan aplikasi PeduliLindungi perlu diperkuat.[49]

Studi ini menemukan dua keterangan yang berbeda terkait kepastian keamanan data dalam aplikasi PeduliLindungi. Keterangan seorang peserta studi mengatakan bahwa Satu Data Vaksinasi maupun PeduliLindungi belum memiliki standar keamanan, sedangkan keterangan lainnya mengatakan bahwa PeduliLindungi telah menggunakan standar yang mengikuti standar Badan Siber dan Sandi Negara (BSSN)[50]. Selain itu, pengumpulan data pribadi di lapangan oleh penyelenggara vaksinasi terkadang masih dilakukan dengan pencatatan secara manual. Contoh-contoh di atas menunjukkan pentingnya pemenuhan standar keamanan data dan pelindungan data oleh aplikasi kesehatan, dibuatnya standar operasional (*standard operating procedure*/SOP) untuk tata kelola data kesehatan, dan pembagian tanggung jawab yang jelas bagi para pemangku kepentingan tata kelola data kesehatan dalam memastikan keamanan dan pelindungan data.[51]

Ke depannya, Kemenkes dibantu oleh Digital Transformation Officer (DTO) berencana untuk mengembangkan PeduliLindungi menjadi aplikasi dengan fitur yang jauh lebih beragam (*super apps*). Namun, mengacu pada landasan hukum PeduliLindungi dalam Keputusan Menteri Komunikasi dan Informatika Nomor 171 Tahun 2020, PeduliLindungi harusnya hanya digunakan pada masa darurat COVID-19. Pengembangan PeduliLindungi sebagai *super apps* memerlukan penjabaran dan pengaturan yang lebih jelas terkait dengan pelindungan data pribadi.

48 Hasil Pertemuan Bilateral dengan Jabar Digital Service (JDS) Provinsi Jawa Barat pada Maret 2022.

49 Esti, K., Novianda, A. H., Suhanda, K. Op.Cit, hal. 56.

50 Ibid.

51 Ibid.

Perluasan penggunaan PeduliLindungi juga menimbulkan risiko bagi Pelindungan Data Pribadi (PDP), terutama prinsip-prinsip keabsahan hukum, transparansi, tujuan yang terbatas, minimalisasi pengumpulan data, dan integritas serta konfidensial. Jika rencana ini direalisasikan, Kemenkes perlu meningkatkan keamanan aplikasi PeduliLindungi dan menyiapkan langkah-langkah mitigasi dalam mengantisipasi kebocoran data pribadi sensitif, seperti NIK.

Di tingkat provinsi, pengelolaan aplikasi kesehatan Pikobar yang dikembangkan Pemprov Jawa Barat dilakukan sepenuhnya oleh Dinas Informasi dan Komunikasi Provinsi Jawa Barat.[52] Saat ini, Pemprov Jawa Barat sedang bekerja sama dengan komunitas IT untuk membangun sistem keamanan Pikobar. Pemanfaatan data aplikasi harus mendapatkan persetujuan pengguna untuk menjamin privasi data.

Rencananya, Pikobar akan dikembangkan menjadi *super apps* dan data yang ada di aplikasi tersebut akan dimanfaatkan untuk keperluan analisis. Hal ini membuat pelindungan keamanan data Pikobar menjadi urgen. Saat ini, aplikasi Pikobar telah memiliki notifikasi kebijakan pelindungan privasi *(privacy notice)* bagi pemilik data. Namun demikian, ketersediaan *privacy notice* ini bervariasi di berbagai fasyankes. Berdasarkan penelitian yang dilakukan oleh CIPG, RSUD Depok mengakui tidak ada notifikasi pelindungan privasi dan data pribadi pada sistem yang digunakan maupun dalam proses pendataan manual. Meski demikian, di Provinsi Jawa Barat, petugas pelayanan kesehatan menyampaikan informasi mengenai siapa pengelola dan pengguna data kepada pemilik data. Sementara itu, di Kota Pontianak, pemberian notifikasi penjagaan privasi dan data pribadi tidak dijalankan dengan seragam. Sebagian mengatakan bahwa notifikasi penjagaan privasi tidak diberikan, meskipun pada praktiknya, petugas pelayanan kesehatan menyampaikan informasi mengenai siapa pengelola dan pengguna data kepada pemilik data.[53]

Mekanisme akuntabilitas

Salah satu aspek yang signifikan dalam tata kelola data di sektor kesehatan selama pandemi adalah penggunaan aplikasi untuk memaksimalkan layanan publik dalam penanggulangan Covid-19 seperti info vaksinasi dan pelacakan kontak. Namun, banyaknya aplikasi yang digunakan dalam input data justru berdampak pada efektivitas implementasi tata kelola data, baik di tingkat pusat maupun daerah yang mengakibatkan kualitas data yang tidak optimal. Data yang tidak berkualitas (misalnya saja, masih tumpang-tindih dan tidak sinkron antara pusat dan daerah) mengakibatkan layanan publik yang terhambat.

Mekanisme akuntabilitas dalam tata kelola data di sektor kesehatan harus dioptimalkan setidaknya pada dua aspek. Aspek pertama adalah mekanisme akuntabilitas dalam memastikan bahwa data kesehatan yang dihasilkan akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar instansi pusat dan instansi daerah melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Referensi dan Data Induk[54]. Data kesehatan yang berkualitas dapat mendorong implementasi kebijakan dan layanan yang tepat guna dan menyasar pihak-pihak yang memang membutuhkan. Sementara aspek kedua berkaitan dengan mekanisme keamanan dan pelindungan data pribadi. Tata kelola data di sektor kesehatan memuat data-data pribadi yang sensitif karena menunjukkan rekam medis seseorang. Tidak ditegakkan prinsip-prinsip pelindungan data pribadi dan keamanan data dapat membahayakan pemilik data.

Seperti yang sudah dijabarkan sebelumnya, proses input dilakukan di level kabupaten/kota. Sementara itu, provinsi memiliki peran dalam melakukan pengawasan dan evaluasi. Namun, karena proses integrasi yang belum berjalan optimal serta kewenangan daerah yang terbatas, masih ditemukan data yang tidak koheren antara pusat dan daerah. Ketidaksesuaian data antara pusat dan daerah ini terutama terjadi di level kabupaten/kota karena beberapa faktor seperti keterbatasan SDM dan infrastruktur. Semenata itu, proses integrasi antara pusat dan daerah juga tidak berjalan optimal. Maka, untuk memastikan data yang dihasilkan akurat dan terpadu, mekanisme akuntabilitas di level daerah dapat dilakukan dengan melibatkan intervensi publik untuk memaksimalkan pelayanan dan memastikan bantuan yang diberikan tepat sasaran.

52 Hasil Pertemuan Bilateral dengan Jabar Digital Service (JDS) pada Maret 2022.

53 Esti, K., Novianda, A. H., Suhanda, K. Op.Cit, hal. 56.

54 Perpres No. 39 Tahun 2019.

Sementara itu, kaitannya dengan keamanan data, pemerintah pusat maupun daerah belum menerapkan Pasal 13 PP 71/2019 yang memuat pentingnya pemberitahuan kepada masyarakat jika terjadi kebocoran data. Pemerintah perlu memahami bahwa mekanisme ini justru mendorong munculnya kepercayaan publik. Dengan adanya pemberitahuan resmi dari pemerintah, masyarakat dapat mengambil keputusan yang tepat sebagai pemilik data. Mekanisme akuntabilitas yang berkaitan dengan keamanan data juga mestinya memastikan mitigasi kebocoran data. Namun, praktik ini, baik di level pusat maupun kabupaten/kota belum diterapkan secara optimal.

Selain itu, dalam penyelenggaran aplikasi kesehatan seperti PeduliLindungi, Silacak, NAR, dan P-Care, pemerintah pusat perlu memberitahukan sejauh mana kerja sama dengan pihak ketiga dalam proses pengembangan aplikasi tersebut. Misalnya saja seperti memastikan batasan kewenangan dan mekanisme pertanggungjawaban pihak eksternal apabila terjadi pelanggaran terhadap keamanan dan privasi data. Penegakan pelindungan privasi data juga dilakukan dengan ketentuan hukum yang berlaku.

4.2. Tata Kelola Data di Sektor Pendidikan

Selain sektor kesehatan, sektor lainnya yang paling terkena dampak penerapan kebijakan pembatasan sosial adalah sektor pendidikan. Pandemi Covid-19 telah mendorong pemerintah untuk melakukan perubahan model pembelajaran dari sistem tatap muka menjadi sistem pembelajaran jarak jauh (PJJ). Tulisan ini akan menjabarkan beberapa persoalan kunci dalam tata kelola data di sektor pendidikan yang mendukung model pembelajaran daring. Persoalan tersebut meliputi kesenjangan pengaturan/regulasi mengenai tata kelola data pendidikan, kurangnya kapasitas kelembagaan, masalah integrasi dan interoperabilitas, kelemahan pada sistem keamanan data dan pengabaian mekanisme akuntabilitas.

Selain dari sisi peraturan, kesenjangan juga tampak pada implementasi tata kelola Dapodik di level nasional dan daerah. Bagian berikut akan menguraikan secara mendetail persoalan tata kelola data di sektor pendidikan.

Kesenjangan antara peraturan-peraturan tata kelola data di sektor pendidikan

Pengaturan mengenai tata kelola data di sektor pendidikan lebih sederhana dan langsung jika dibandingkan dengan pengaturan di sektor kesehatan. Pada sistem pendidikan nasional, data memegang peranan krusial dalam penyusunan program perencanaan pendidikan. Dibutuhkan data yang akurat, lengkap, mutakhir, valid serta dapat dipertanggungjawabkan guna menjamin kualitas pendidikan nasional.

Untuk itu, pemerintah membangun sistem pendataan berskala nasional yang disebut dengan Data Pokok Pendidikan (Dapodik), yang diatur dalam Peraturan Menteri Pendidikan dan Kebudayaan Nomor 79 Tahun 2015 tentang Data Pokok Pendidikan. Dapodik berisi data siswa, guru, sekolah, hingga kurikulum. Selain Dapodik, data pendidikan juga bersumber dari pangkalan data pendidikan tinggi yang diatur pada Peraturan Menteri Riset, Teknologi dan Pendidikan Tinggi Nomor 61 Tahun 2016 tentang Pangkalan Data Pendidikan Tinggi (PDDIKTI). Baik Dapodik maupun data Dikti, pengelolaannya bersifat *bottom-up*. Namun kertas kebijakan ini akan fokus membahas tata kelola Dapodik.

Dapodik adalah suatu sistem pendataan terpadu dan merupakan sumber data utama pendidikan nasional. Selain menunjang penyusunan program-program pembangunan pendidikan yang terarah, Dapodik mempermudah proses pemantauan dan evaluasi implementasi program. Pengelolaan Dapodik dilakukan oleh Pusat Data dan Informasi (Pusdatin) Kemendikbud Ristek sebagai walidata, bertugas merancang basis pendataan dan melakukan pengelolaan, verifikasi, validasi dan integrasi data pendidikan.[55]

Di tingkat daerah, Dinas Pendidikan berperan sebagai pengguna data dan koordinator yang melakukan sosialisasi dan bimbingan pelayanan teknis, mengelola manajemen pendataan, memanfaatkan data yang dihasilkan dari Dapodik, mengalokasikan anggaran yang mendukung pendataan melalui Dapodik, serta bertugas memastikan akurasi data yang dikumpulkan oleh satuan pendidikan (sekolah) dan dan dikirimkan tepat waktu. Sekolah merupakan produsen data yang melakukan pengumpulan dan pemutakhiran data

55 Permendikbud Ristek No. 28 Tahun 2021 tentang Organisasi dan Tata Kerja Kemendikbud Ristek, Pasal 288.

secara berkala dan langsung di sistem pusat Dapodik yang dikelola oleh Pusdatin Kemendikbud Ristek.[56]

Terdapat operator data di Dinas Pendidikan dan Kebudayaan yang bertugas memastikan akurasi data yang dimasukkan oleh satuan pendidikan pada sistem Dapodik, namun tidak memiliki akses terhadap sistem Dapodik. Akses langsung untuk Dapodik hanya dimiliki oleh sekolah, di mana setidaknya terdapat satu orang operator yang bertugas memasukkan data sekolah ke dalam sistem Dapodik. Dari mekanisme tersebut, dapat dikatakan bahwa hubungan antara pemerintah pusat dan daerah secara struktur memang jauh, namun dekat secara sistem.[57]

Secara umum, Dapodik berfungsi untuk:[58]

- Pengalokasian dana bantuan operasional sekolah (BOS) bagi satuan pendidikan sesuai dengan jumlah peserta didik yang dimiliki.
- Pengalokasian kuota penerima tunjangan bagi para tenaga pendidik yang telah memenuhi syarat.
- Pengalokasian bantuan untuk perbaikan sarana dan prasarana bagi sekolah yang belum memiliki fasilitas memadai.
- Pengajuan dan perbaikan data kelembagaan sekolah.
- Pengajuan dan verifikasi dan validasi data dan Nomor Unik Pendidik dan Tenaga Kependidikan (NUPTK).
- Pengajuan dan verifikasi dan validasi data peserta didik dan Nomor Induk Siswa Nasional (NISN).
- Pengajuan dan verifikasi dan validasi data satuan pendidikan dan Nomor Pokok Sekolah Nasional (NPSN).
- Pemetaan dan pemerataan jumlah tenaga pendidik.
- Melaksanakan pemantauan dan evaluasi terhadap kebijakan-kebijakan dan program-program pendidikan nasional.
- Percepatan dan peningkatan efektivitas pelaporan yang dilaksanakan dari satuan pendidikan hingga kementerian, serta meminimalisasi risiko pelanggaran.

Guna melakukan fungsi-fungsi tersebut, tata laksana Dapodik ditunjang dengan inisiasi *e-government* sebagaimana dirumuskan pada Perpres 95/2018, Perpres 39/2019 dan PP 71/019. Sebagaimana telah dijabarkan pada bagian sebelumnya, ketiga peraturan tersebut menjadi acuan pelaksanaan tata kelola data di tingkat nasional.[59] Secara khusus, Perpres 95/2018 telah memasukkan prinsip keamanan di dalam pelaksanaannya, yang menjadi tanggung jawab Badan Siber dan Sandi Negara (BSSN) untuk menjamin keamanan SPBE tersebut.[60]

Penyelenggaraan Dapodik harus sejalan dengan prinsip-prinsip yang tercantum dalam peraturan-peraturan tersebut, seperti keterpaduan, akuntabilitas, interoperabilitas, keamanan, standar data dan metadata, dan efektivitas. Namun, Permendikbud 79/2015 yang terbit sebelum peraturan tentang SPBE, Satu Data dan PSTE tidak secara spesifik memasukkan prinsip-prinsip tersebut. Untuk memastikan harmonisasi peraturan, perlu dilakukan perubahan terhadap Permendikbud Dapodik.

Merespons hal tersebut, saat ini, Kemendikbud Ristek tengah dalam proses mengakomodasi perubahan Permendikbud 79/2015 yang akan digantikan dengan Rancangan Peraturan Menteri tentang Satu Data Pendidikan.[61] Rancangan peraturan tersebut merupakan turunan dari Perpres SPBE dan Satu Data, sehingga akan memasukkan semua prinsip-prinsip tata kelola data yang baik dan diharapkan dapat menjawab persoalan tata kelola data pendidikan nasional. Selain itu, rancangan peraturan juga akan memasukkan jaringan analisis penelitian untuk pemanfaatan penggunaan data.[62]

Kemudian dengan adanya otonomi daerah, pemerintah daerah memiliki otoritas untuk membuat peraturan pelaksana di tingkat provinsi dan kabupaten/kota berupa peraturan/keputusan gubernur atau peraturan bupati/walikota[63] terkait pelaksanaan Dapodik. Peraturan daerah tersebut biasa dikeluarkan pada awal tahun anggaran dengan melihat kebutuhan

56 Permendikbud No. 79 Tahun 2015 tentang Data Pokok Pendidikan, Pasal 12-14.

57 Hasil Pertemuan Bilateral dengan Analis Kebijakan Kemendikbud Ristek pada Januari 2022.

58 BP PAUD dan Dikmas NTT, Data Pokok Pendidikan (Dapodik), 30 Oktober 2019. Diakses di https://bppauddikmasntt.kemdikbud.go.id/index.php/ult/11-artikel/59-data-pokok-pendidikan-dapodik

59 Esti, K., Novianda, A. H., Suhanda, K. Op.Cit.

60 Lampiran Perpres No. 95 Tahun 2018.

61 Lihat Kepmendikbud Ristek No. 190/P/2021 tentang Perubahan atas Keputusan Menteri Pendidikan dan Kebudayaan No. 69/P/2021 tentang Program Penyusunan Peraturan Menteri Pendidikan dan Kebudayaan Tahun 2021.

62 Hasil Pertemuan Bilateral dengan Pusdatin Kemendikbud Ristek pada Februari 2022.

63 Hasil Pertemuan Bilateral dengan Dinas Pendidikan Jawa Barat dan Dinas Pendidikan Pontianak pada Maret - April 2022.

alokasi anggaran Dapodik di masing-masing daerah. Dapodik di tingkat daerah belum dijadikan dasar pengambilan keputusan, sehingga banyak kebijakan pendidikan di daerah yang diambil tidak berbasis data dan belum sejalan dengan kebijakan pusat mengenai perencanaan pendidikan.[64]

Berbeda dengan tata kelola data pada sektor kesehatan, pelaksanaan Dapodik di tingkat daerah tetap mengacu pada Permendikbud 79/2015 untuk penggunaan data yang seragam menuju integrasi manajemen data. Sementara peraturan di tingkat daerah hanya mengatur pendanaan untuk merespons kebutuhan program pendidikan di daerah seperti bantuan operasional sekolah (BOS).

Sehubungan dengan keamanan data, Permendikbud 79/2015 juga belum secara terperinci memasukkan mekanisme pengamanan data, hanya mewajibkan setiap orang yang memiliki akses penggunaan Dapodik untuk menjaga kerahasiaan dan keamanan data. Dan apabila terjadi pelanggaran keamanan akan dikenakan sanksi sesuai peraturan yang berlaku.[65] Ketentuan tersebut berkaitan dengan prinsip pelindungan data pribadi, di mana Pasal 17 secara implisit mengikutsertakan prinp integritas dan konfidensial serta prinsip integritas di dalamnya. Kemendikbud Ristek yang saat ini dalam proses penyusunan Rancangan Peraturan Menteri tentang Satu Data Pendidikan sebaiknya memasukkan mekanisme tentang perlindungan terhadap kerahasiaan data secara spesifik, atau setidaknya tertuang dalam peraturan turunan yang lebih teknis.

Kapasitas kelembagaan: kurangnya kapasitas personel

Salah satu elemen kunci dalam tata pemerintahan yang baik adalah manusia. Sebab itu penting untuk memastikan kapasitas personel yang berwenang dalam pemrosesan data memiliki pemahaman dan pengetahuan yang baik mengenai data. Dalam konteks Dapodik yang tersentralisasi, agar pemahaman tentang data merata dan seragam harus dilakukan baik secara horizontal (di lingkup Kemendikbud Ristek) maupun vertikal (dari level kementerian, dinas provinsi dan kabupaten/kota, hingga sekolah).

Setiap sekolah memiliki operator data yang bertugas melakukan pengumpulan dan pemutakhiran data, namun belum diimbangi dengan pengetahuan yang komprehensif mengenai alur data dan sistem Dapodik. Masih ditemukan perbedaan pemahaman mengenai definisi data dan metadata, serta tentang peran dan tanggung jawab penyelenggara Dapodik pada operator data sekolah.[66] Perbedaan tersebut perlu dijembatani, misalnya dengan memberikan pelatihan secara berkala tentang Dapodik bagi para operator, termasuk mensosialisasikan updating informasi Dapodik. Dengan demikian, pemahaman yang sama dan merata tentang elemen-elemen Dapodik dapat menjadi pondasi tata kelola data yang kuat.

Secara khusus, pengetahuan dan kesadaran tentang pelindungan data pribadi dan sensitif juga masih minim, tidak saja di tingkat satuan pendidikan namun hingga kementerian. Padahal banyaknya data pribadi dan sensitif yang diproses dalam Dapodik seperti seperti data anak/peserta didik, membuat hal ini penting menjadi perhatian para pihak penyelenggara data di level pusat dan daerah. Permendikbud 79/2015 belum mengatur secara spesifik tentang keamanan data dan perlindungan data pribadi bisa jadi akar masalah pelaksanaan di daerah. Sehingga perlu panduan atau standar yang jelas dan mudah dilaksanakan oleh operator data tentang bagaimana data pribadi dan sensitif tersebut akan digunakan.

Selain persoalan mengenai kompetensi personel, terbatasnya jumlah SDM juga berdampak pada kualitas data yang dihasilkan. Terutama sejak pandemi melanda, tenaga pendidik dan kependidikan mendapat tambahan tugas untuk menjadi operator data ke dalam sistem Dapodik. Masalah jumlah SDM disebabkan oleh keterbatasan sumber pendanaan untuk merekrut operator Dapodik sesuai dengan jumlah dan kompetensi yang dibutuhkan mendorong Dinas Pendidikan dan Kebudayan banyak mempekerjakan pegawai honorer yang sering berganti-ganti. Hal tersebut berakibat pada rendahnya kualitas data yang dihasilkan dan belum memenuhi kebutuhan.[67]

Baik Kemendikbud Ristek maupun Dinas Pendidikan perlu secara khusus menyiapkan program peningkatan

64 Hasil Pertemuan Bilateral dengan Pusdatin Kemendikbud Ristek pada Februari 2022.

65 Permendikbud No. 79 Tahun 2015, Pasal 17 ayat (1) dan (2).

66 Esti, K., Novianda, A. H., Suhanda, K. Op.Cit.

67 Hasil Pertemuan Bilateral dengan Dinas Pendidikan Jawa Barat dan Dinas Pendidikan Pontianak pada Maret - April 2022.

kapasitas bagi para operator data di tingkat daerah, bisa dengan melanjutkan bimbingan teknis secara regular dan menambah materi tentang literasi data, alur pendataan, pemantauan dan evaluasi, serta pelindungan data pribadi. Selain itu dibutuhkan sosialisasi untuk menyeragamkan definisi dan pemahaman mengenai peran operator di lapangan serta pentingnya pemanfaatan dapodik untuk pembangunan daerah. Kegiatan-kegiatan tersebut bisa menjadi bagian dari rencana anggaran dapodik di daerah agar menjamin kualitas personel dapodik di lapangan dan terbangunnya sistem pendidikan yang lebih kokoh.

Persoalan interoperabilitas dan integrasi data

Prinsip interoperabilitas (bagi pakai) yang belum tercantum secara spesifik dalam pengaturan mengenai Dapodik juga termanifestasi dalam praktik pengelolaannya. Di lingkup internal kementerian pun akses terhadap Dapodik sangat terbatas, hanya bisa diakses oleh Pusdatin. Apabila direktorat atau bagian lain ingin menarik dapodik untuk dapat digunakan, harus mengajukan permohonan akses ke Pusdatin, dan data yang bisa diakses juga dibatasi.[68]

Begitupun dengan Dinas Pendidikan selaku koordinator yang memastikan sekolah melakukan pengisian Dapodik, memiliki akses yang sangat terbatas ke sistem Dapodik, di mana mereka harus mengajukan permohonan ke Pusdatin Kemendikbud Ristek untuk mendapatkan data yang dibutuhkan di wilayahnya. Padahal hasil pengumpulan data melalui Dapodik menjadi dasar diterbitkannya data statistik pendidikan yang memberikan akses informasi kepada para pemangku kepentingan.[69]

Kemendikbud Ristek sebagai institusi tunggal yang diamanatkan untuk mengelola Dapodik belum optimal menjalankan mekanisme bagi pakai data lintas sektor. Idealnya, pelaksanaan *e-government* yang mengutamakan prinsip keamanan dan interoperabilitas diharapkan dapat meningkatkan interaksi antara pemerintah dan masyarakat sehingga mampu mendorong perkembangan sosial ekonomi. Pembatasan kewenangan untuk mengakses Dapodik tersebut merupakan strategi pengamanan data yang dinilai Kemendikbud Ristek sudah sejalan dengan prinsip-prinsip pelindungan data pribadi pada Perpres SPBE, Perpres Satu Data dan PP PSTE. Hal tersebut dapat dipahami sebab dalam proses bagi pakai data pembatasan akses terhadap data pribadi dan sensitif menjadi penting.

Namun mekanisme yang terpusat membuat konsep interoperabilitas tidak dapat dijalankan secara optimal dan menyulitkan pemerintah daerah dalam mendukung pelaksanaan dan pemanfaatan Dapodik di wilayahnya. Sebab Dapodik yang dikelola oleh pemerintah pusat tidak sepenuhnya menggambarkan kondisi di setiap daerah, sementara terdapat kebutuhan data yang akurat dan riil untuk menggambarkan situasi di setiap daerah yang berbeda-beda. Oleh karena itu, Dinas Pendidikan juga melakukan pengumpulan data sendiri untuk memenuhi kebutuhannya, misalnya data mengenai SDM tenaga pendidik, akses pendidikan dan fasilitas sekolah di wilayahnya.[70]

Sekolah sebagai operator Dapodik juga memiliki akses yang terbatas, hanya bisa melihat data sekolah yang mereka miliki saja. Di samping itu, mereka juga harus melakukan pengisian data pada sistem terpisah yang dibutuhkan oleh Dinas Pendidikan dan Kebudayaan di daerahnya. Tugas tersebut jelas menambah berat kerja mereka sebagai tenaga pendidik sehingga sering ditemui input data yang berulang dan tidak sinkron pada prosesnya. Dengan berbagai macam sistem informasi yang tersedia secara sporadis dalam berbagai sistem dan regulasi, integrasi data masih menjadi pekerjaan rumah besar bagi pemerintah dalam rangka meningkatkan mutu pelayanan publik.

Berkaitan dengan integrasi data, sistem Dapodik belum sepenuhnya terintegrasi karena masih terdapat perbedaan sehingga validasi data belum terjamin. Sebagai contoh, Dapodik belum sinkron dengan data NIK yang dikelola oleh Ditjen Dukcapil Kemendagri. Sedangkan dalam proses integrasi data harus terdapat proses verifikasi dan validasi, baik secara eksternal maupun internal.

Kendala integrasi juga ditemukan karena *cut off* data yang dilakukan setahun sekali, membuat Dapodik tidak selalu *real-time* dan akurat. Apabila input data dilakukan dengan benar pada sistem Dapodik

68 Hasil Pertemuan Bilateral dengan Analis Kebijakan Kemendikbud Ristek pada Januari 2022.

69 Dirjen PAUD PM, Panduan Aplikasi Dapodik Versi 2021. Diakses di https://cdn-dapodik.kemdikbud.go.id/panduan/Panduan_Aplikasi_Dapodikdasmen_Versi_2021.pdf

70 Hasil Pertemuan Bilateral dengan Dinas Pendidikan Jawa Barat pada Maret 2022.

maka pemetaan kebutuhan pendidikan akan sesuai dengan keadaan sebenarnya. Namun jika input data tidak dilakukan tepat waktu dapat berdampak buruk bagi sekolah, jika operator melakukan input dan sinkronisasi setelah jadwal yang ditetapkan maka sekolah tidak akan mendapatkan bantuan.

Sistem Dapodik bersifat semi daring, dengan harapan sekolah tetap dapat memasukkan data walau tanpa jaringan internet, internet hanya dibutuhkan ketika sinkronisasi atau pengambilan data. Namun pada praktiknya, *server* Dapodik sering mengalami kegagalan fungsi karena mengalami perbaikan sistem pada setiap semester tahun ajaran sehingga susah diakses. Setiap perubahan pada sistem berarti terdapat perubahan komponen pengisian data. Perubahan yang cepat menuntut operator untuk terus meningkatkan kemampuannya ketika melakukan input Dapodik.

Interoperabilitas dan integrasi data tentu harus didukung dengan infrastruktur yang baik dan merata agar fungsi pengelolaan data pendidikan di daerah, terutama kabupaten/kota dapat berjalan maksimal. Tidak semua wilayah memiliki sumber daya yang memadai, sehingga pemerintah harus memastikan sekolah memiliki fasilitas yang cukup untuk melakukan input data, koneksi internet yang stabil dan memiliki akses ke server Dapodik.

Keamanan dan privasi data

Situasi pandemi menuntut tingginya aktivitas sistem dan transaksi elektronik yang mensyaratkan pertukaran data yang cepat namun kerap mengabaikan prinsip keamanan. Pada praktik pengelolaan Dapodik misalnya, dalam kurun dua tahun pandemi di Indonesia, setidaknya terjadi dua kasus kebocoran data guru dan hingga kini belum diketahui dengan pasti bagaimana penyelesaian kasus tersebut.[71]

Sebagai upaya mengimplementasikan mandat Perpres SPBE terkait keamanan, pada Agustus 2020 Kemendikbud meresmikan Education Computer Security Incident Response Team (EduCSIRT) dengan visi untuk mewujudkan ketahanan siber pada sektor pendidikan yang andal dan profesional. Sementara misi EduCSIRT adalah:[72]

- mengoordinasikan dan mengolaborasikan layanan keamanan siber pada sektor pemerintah khususnya sektor pendidikan baik internal dan eksternal;
- mengidentifikasi kerentanan keamanan secara menyeluruh;
- meningkatkan respons aspek keamanan kepada seluruh satuan kerja Kemendikbud;
- meningkatkan mutu layanan TIK pendidikan dan kebudayaan dari ancaman siber.

EduCSIRT memberikan layanan dengan menyajikan data statistik mengenai insiden yang terjadi pada sektor pemerintah sebagai bentuk sentra informasi keamanan siber serta respons insiden dalam bentuk triase insiden, koordinasi insiden, dan resolusi insiden. Di mana salah komponen dari resolusi insiden adalah melakukan investigasi dan dampak insiden.[73] Namun pada kasus kebocoran data yang terjadi, EduCSIRT belum menunjukkan upaya yang berarti.

Praktik bagi pakai dapodik yang masih terbatas juga belum sepenuhnya menjamin keamanan data. Di tingkat daerah misalnya, karena kebutuhan pertukaran data yang cepat maka data disimpan dalam format excel dan dikirimkan melalui WhatsApp dengan alasan efisiensi. Proses tersebut jelas tidak mempertimbangkan risiko kebocoran data, sebab data dapat dengan mudah tersebar ke pihak-pihak yang tidak memiliki kewenangan dan tanggung jawab.

Meskipun payung hukum pelindungan data pribadi di Indonesia belum disahkan, namun penerapan prinsip-prinsipnya telah dapat dilaksanakan. Praktik baik ini sudah dijalankan oleh Dinas Pendidikan dan Kebudayaan di beberapa daerah, di mana data yang dipublikasi untuk masyarakat adalah data yang telah difilter dan tidak mengekspos data sensitif. Meskipun secara institusional pemahaman personel mengenai pelindungan data pribadi belum merata.[74] Sistem keamanan yang dikembangkan bersama dengan pihak ketiga juga dikontrol secara berkala dan dilakukan reset ketika perjanjian kerjasama dengan pihak ketiga tersebut berakhir. Untuk itu, pemerintah perlu membangun sistem keamanan yang baik, tidak hanya peraturan namun juga implementasinya.

---

71 Lihat tautan berita tentang bocornya data guru pada tahun 2020 dan 2021 https://finance.detik.com/berita-ekonomi-bisnis/d-5263052/gawat-data-guru-honorer-calon-penerima-blt-gaji-diduga-bocor
https://regional.kompas.com/read/2021/11/09/113200978/fakta-data-815-guru-di-banten-bocor-pelaku-ternyata-orang-dalam-diperiksa?page=all

72 EduCSIRT Kemendikbud Ristek, Profil. Diakses di https://educsirt.kemdikbud.go.id/portal/profil

73 EduCSIRT Kemendikbud Ristek, Aduan Siber. Diakses https://educsirt.kemdikbud.go.id/portal/aduan

74 Hasil Pertemuan Bilateral dengan Dinas Pendidikan Jawa Barat pada Maret 2022.

Mekanisme akuntabilitas

Sentralisasi pengelolaan data yang prosesnya tertutup berujung pada tidak transparannya penggunaan data. Pada sektor pendidikan, Dapodik memuat banyak data pribadi dan sensitif yang perlu dilindungi dan harus terdapat penjaminan terhadap keamanan data tersebut. Permendikbud 79/2015 mengatur bahwa setiap pelanggaran terhadap kerahasiaan dan keamanan data akan dikenakan sanksi sesuai ketentuan perundang-undangan, meski tidak terdapat penjelasan lebih lanjut ketentuan mana yang dijadikan rujukan.[75]

Selain Permendikbud, pengaturan tentang penjaminan keamanan data secara implisit tercermin dalam Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional dan Permendikbud Nomor 10 Tahun 2017 tentang Perlindungan bagi Pendidik dan Tenaga Kependidikan di mana pendidik dan tenaga pendidikan berhak mendapatkan perlindungan hukum, profesi, keselamatan dan kesehatan kerja, serta hak atas kekayaan intelektual di dalam menjalankan tugasnya.[76] Mengacu pada kebijakan tersebut, maka pendidik dan kependidikan yang dirugikan dari kasus kebocoran data guru honorer beberapa waktu lalu, berhak mendapatkan perlindungan hukum, setidaknya melalui proses hukum.

Oleh karena di dalam penyelenggaran Dapodik banyak bekerja sama dengan pihak ketiga, pemerintah pusat dan lokal harus memastikan batasan kewenangan dan mekanisme pertanggungjawaban pihak eksternal tersebut apabila terjadi pelanggaran terhadap keamanan dan privasi data, termasuk penegakan sanksi secara tegas sesuai dengan ketentuan yang berlaku. Selain itu, bisa pula dengan membuat akses berjenjang atau berlapis bagi para pihak yang terlibat dalam pengelolaan dapodik guna meminimalisasi kebocoran data pribadi.

Selain mekanisme pertanggungjawaban, praktik tata kelola data juga mengharuskan adanya pemantauan dan evaluasi untuk melihat sejauh apa keberhasilan suatu proses. Permendikbud 79/2015 memasukkan ketentuan tentang perlunya dilakukan evaluasi secara berkala untuk perbaikan sistem Dapodik dan proses bisnisnya. Namun, proses ini hanya melibatkan internal Kemendikbud, sehingga memiliki potensi bias yang besar. Di lain sisi, UU 20/2003 menyatakan bahwa masyarakat juga dapat berpartisipasi dalam peningkatan mutu pelayanan pendidikan yang meliputi perencanaan, pengawasan, dan evaluasi program pendidikan.[77] Guna menjamin bahwa proses tata kelola Dapodik lebih transparan, pemerintah pusat dan daerah harus lebih memperhatikan persoalan di lapangan serta melibatkan partisipasi publik di dalam proses pengambilan kebijakan.

5. Simpulan dan Rekomendasi

Pandemi telah mendorong eskalasi transformasi digital dalam berbagai sektor, termasuk kesehatan dan pendidikan. Pada prinsipnya, transformasi digital seyogianya meningkatkan kualitas penyelenggaraan tata kelola data. Namun, pada praktiknya, ketersediaan kerangka hukum dan infrastruktur digital, kapasitas kelembagaan, sistem informasi, dan pelindungan keamanan dan privasi data menjadi tantangan bagi upaya mewujudkan tata kelola data yang efektif.

a. Kerangka hukum

Ketersediaan kerangka peraturan tata kelola data yang memadai penting bagi penyelenggaraan tata kelola data yang optimal. Kajian ini menemukan adanya kebutuhan untuk mengharmonisasi peraturan-peraturan yang menjadi landasan penyelenggaraan tata kelola data di Indonesia. Selain itu, untuk mengatasi kesenjangan antara ketersediaan peraturan dan kebutuhan praktis pengaturan di lapangan, peraturan-peraturan turunan, seperti panduan atau petunjuk pelaksanaan, perlu dibuat. Dalam pembuatan peraturan-peraturan turunan ini, pemerintah perlu memastikan bahwa prinsip-prinsip tata kelola data yang terdapat pada Perpres SBPE, Perpres Satu Data, dan PP PSTE dan prinsip-prinsip pelindungan data pribadi diintegrasikan.

Praktik sentralisasi dan desentralisasi tata kelola data di sektor kesehatan dan pendidikan berimplikasi pada perbedaan implementasi tata kelola data yang berbeda di tingkat pusat dengan daerah. Guna menghindari tumpang tindih tanggung jawab antarpemangku kepenting-

75 Permendikbud No. 79 Tahun 2015, Pasal 17 ayat (2).

76 UU No. 20 Tahun 2003, Pasal 40 ayat (1) dan Permendikbud No. 10 Tahun 2017, Pasal 2.

77 UU No. 20 Tahun 2003 tentang Sistem Pendidikan Nasional, Pasal 56 ayat (1).

an yang terlibat dalam pengelolaan sistem informasi kesehatan dan pendidikan, diperlukan harmonisasi peraturan lintas tingkat administrasi di masing-masing sektor dan penguatan koordinasi antarpengelola data di tingkat nasional, provinsi, dan kabupaten/kota.

Terkait pelindungan data pribadi, pemetaan aktor-aktor yang terlibat dalam tata kelola data di sektor privat dan publik maupun di tingkat pusat dan daerah perlu dilakukan guna mengidentifikasi peran, tanggung jawab, dan alur koordinasi antaraktor yang perlu diatur melalui peraturan-peraturan pelindungan data pribadi.

b. Kapasitas institusional

Pemerintah harus mempertimbangkan bahwa penggunaan aplikasi alih-alih memperbaiki sistem yang ada dapat mengeksklusi kelompok marjinal, misalnya kelompok masyarakat yang hidup di daerah dengan koneksi internet yang minim dan kelompok masyarakat yang kurang terampil menggunakan teknologi digital. Oleh karena itu, diperlukan mekanisme tata kelola data yang holistik dan inklusif dalam implementasinya. Hal ini dapat dilakukan, misalnya, dengan menyiapkan infrastruktur maupun sarana-prasarana terkait yang dapat digunakan oleh warga yang tidak memiliki ponsel. Peningkatan sarana-prasarana ini juga harus disertai dengan kemahiran dan kecakapan petugas pengendali/pemroses data dalam mengoperasikan aplikasi. Dengan demikian, pemerintah pusat perlu memberikan pelatihan yang terintegrasi dan berkelanjutan kepada petugas.

Pentingnya peran operator data dalam penyelenggaraan pelayanan publik di sektor kesehatan dan pendidikan tidak terlepas dari peran serta pemerintah daerah di dalamnya. Untuk dapat menggambarkan ciri khas situasi di masing-masing daerah, setidaknya pemerintah daerah perlu diberikan kewenangan untuk dapat mengakses dan menggunakan data yang dibutuhkan di daerahnya.

Peningkatan kapasitas berkelanjutan untuk semua pihak yang terlibat dalam penyelenggaraan tata kelola data penting untuk meningkatkan pemahaman mereka terkait alur data, prinsip-prinsip tata kelola data yang baik, dan pemanfaatan data untuk pelayanan publik. Operator data perlu memiliki pemahaman tentang pelindungan data pribadi dan kompetensi teknis untuk memastikan data pribadi dan data sensitif terlindungi. Untuk menunjang hal tersebut, diperlukan pemerataan infrastruktur tata kelola data di seluruh daerah di Indonesia.

c. Integrasi dan interoperabilitas data

Persoalan integrasi data merupakan pekerjaan rumah besar yang belum terselesaikan hingga kini. Untuk mewujudkan sistem yang terintegrasi dan dapat dibagi-pakaikan lintas sektor, hal fundamental yang harus dilakukan oleh pemerintah ialah mengenyampingkan ego sektoral dan membangun kepercayaan antara pemerintah pusat dan daerah. Menciptakan kolaborasi lintas sektor diperlukan agar tata kelola data lebih holistik, berkelanjutan dan inklusif. Integrasi juga dapat dicapai dengan menyeragamkan standar-standar data di tingkat pusat dan daerah agar akurasi dan validasi data lebih terjamin.

d. Keamanan data dan Pelindungan Data Pribadi

Meningkatnya risiko kebocoran data selama pandemi Covid-19 menuntut pemerintah untuk mengembangkan sistem keamanan data yang lebih baik. Agar dapat meminimalisasi potensi kebocoran data, penting untuk menyusun peta jalan mitigasi kebocoran data untuk sektor kesehatan dan pendidikan di tingkat nasional dan lokal. Tidak saja soal kerahasiaan dan keamanan, pengelolaan data juga perlu menetapkan batasan akses terkait pemrosesan data pribadi. Akses dapat dibuat berjenjang sesuai dengan tugas dan fungsi personel dalam tata kelola data. Untuk membangun peta jalan ini, tugas besar pemerintah adalah melakukan integrasi dan kolaborasi antar kementerian/lembaga untuk mewujudkan data terintegrasi yang bisa dibagi-pakaikan oleh semua sektor dan memastikan diterapkannya prinsip-prinsip pelindungan data pribadi.

e. Mekanisme akuntabilitas

Berkaitan dengan penjaminan terhadap keamanan dan privasi data, pemerintah perlu memastikan bahwa mekanisme akuntabilitas tata kelola data diselenggarakan sesuai dengan peraturan perundang-undangan yang berlaku. Untuk memastikan tata kelola data berjalan sebagaimana ditetapkan oleh peraturan perundangan-undangan, perlu ditegaskan secara rinci bentuk-bentuk pertanggung-jawaban lembaga atau personel dalam hal keamanan data, terutama ketika terjadi kebocoran data.

Mekanisme akuntabilitas juga harus dapat melindungi operator data di lapangan dari pihak-pihak yang tidak bertanggung jawab. Ketika kebocoran data terjadi, investigasi harus dilakukan secara komprehensif dan hingga tuntas sesuai dengan ketentuan perundang-undangan yang berlaku, hal tersebut merupakan bentuk pertanggungjawaban pemerintah dalam pelayanan publik kepada masyarakat.

REFERENSI

ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN). 2012. *Framework on Personal Data Protection*. https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

Azzahra, Nadia Fairuza. 2020." Mengkaji Hambatan Pembelajaran Jarak Jauh di Indonesia di Masa Pandemi Covid-19". *Seri Ringkasan Kebijakan*, No. 2. https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_beb2bbe622c241409452fe6803a410f0.pdf

BP PAUD dan Dikmas NTT. 2019. *Data Pokok Pendidikan (Dapodik)*. https://bppauddikmasntt.kemdikbud.go.id/index.php/ult/11-artikel/59-data-pokok-pendidikan-dapodik

Databoks. 2020. *Ini Rasion Tempat Tidur Rumah Sakit 34 Provinsi di Indonesia*. Diakses 2 April 2022. https://databoks.katadata.co.id/datapublish/2020/03/30/ini-rasio-tempat-tidur-rumah-sakit-34-provinsi-di-indonesia

Data Governance Institute, *Defining Data Governance*. https://datagovernance.com/defining-data-governance/

ELSAM. 2018. *Undang-Undang Pelindungan Data Pribadi Penting Segera Diwujudkan, Siaran Pers, 7 Maret 2018*. https://elsam.or.id/uu-perlindungan-data-pribadi-penting-segera-diwujudkan/

Eryurek, Evren. et.al. 2021. Data Governance, *The Definitive Guide: People, Processes, and Tools to Operationalise Data Trustworthiness*. O'Reilly

Esti, K., Novianda, A. H., Suhanda, K. (2022). Menata Kelola Data demi Pelayanan Publik: Studi Kasus Tata Kelola Data Sektor Kesehatan dan Pendidikan di Indonesia selama Pandemi Covid-19. Jakarta: Centre for Innovation Policy and Governance dan Yayasan Tifa.

ICW. 2021. *Percepatan Penyaluran Insentif dan Santunan Tenaga Kerja Kesehatan dalam Penanganan Covid19*. https://antikorupsi.org/sites/default/files/dokumen/Policy%20Brief%20Insentif%20Nakes_FINAL_compressed.pdf

Indonesia. 2003. *Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional*. Jakarta.

Indonesia. 2008. *Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik*. Jakarta.

Indonesia. 2009. *Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan*. Jakarta.

Indonesia. 2014. *Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan*. Jakarta.

Indonesia. 2016. *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Jakarta.

Indonesia. 2014. *Peraturan Pemerintah Nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan*. Jakarta.

Indonesia. 2017. *Peraturan Pemerintah Nomor 46 Tahun 2017 tentang Strategi e-Kesehatan Nasional*. Jakarta.

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

Indonesia. 2018. *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*. Jakarta.

Indonesia. 2019. *Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia*. Jakarta.

Kementerian Kesehatan. *Peraturan Menteri Kesehatan Nomor 97 Tahun 2015 tentang Peta Jalan Sistem Informasi Kesehatan 2015-2019*. Jakarta.

Kementerian Komunikasi dan Informatika. *Keputusan Menteri Komunikasi dan Informatika Nomor 171 Tahun 2020 tentang tentang Penetapan Aplikasi Pedulilindungi Dalam Rangka Pelaksanaan Surveilans Kesehatan Penanganan Covid-19*. Jakarta.

Kementerian Komunikasi dan Informatika. *Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*. Jakarta.

Kementerian Pendidikan dan Kebudayaan. 2015. *Peraturan Menteri Pendidikan dan Kebudayaan Nomor 79 Tahun 2015 tentang Data Pokok Pendidikan*. Jakarta.

Kementerian Pendidikan dan Kebudayaan. 2017. *Peraturan Menteri Pendidikan dan Kebudayaan Nomor 10 Tahun 2017 tentang Perlindungan bagi Pendidik dan Tenaga Kependidikan*. Jakarta.

Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi. 2021. *EduCSIRT*.

Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi. 2021. *Keputusan Menteri Pendidikan, Kebudayaan, Riset dan Teknologi Nomor 190/P/2021 tentang Perubahan atas Keputusan Menteri Pendidikan dan Kebudayaan No. 69/P/2021 tentang Program Penyusunan Peraturan Menteri Pendidikan dan Kebudayaan Tahun 2021*. Jakarta.

Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi. 2021. *Peraturan Menteri Pendidikan, Kebudayaan, Riset dan Teknologi Nomor 28 Tahun 2021 tentang Organisasi dan Tata Kerja Kemendikbud Ristek*. Jakarta.

Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi: Direktorat Jenderal Pendidikan Anak Usia Dini, Pendidikan Dasar, Dan Pendidikan Menengah. 2021. *Panduan Aplikasi Dapodik Versi 2021*. https://cdn-dapodik.kemdikbud.go.id/panduan/Panduan_Aplikasi_Dapodikdasmen_Versi_2021.pdf

Kota Pontianak. 2021. *Peraturan Walikota Nomor 46 Tahun 2021 tentang Satu Data Kota Pontianak*. Pontianak.

Lewis, Lori. 2021. *Infographic: What Happens In An Internet Minute 2021*. https://www.allaccess.com/merg Seae/archive/32972/infographic-what-happens-in-an-internet-minute

Medcom.id. 2021. *Indonesia Masih Kekurangan SDM Kesehatan*. Diakses 2 April 2022. https://www.medcom.id/nasional/politik/5b2Glxnk-indonesia-masih-kekurangan-sdm-kesehatan

OECD. 2013. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD. 2013. *Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges*. OECD Publishing. http://dx.doi.org/10.1787/9789264193505-en

OECD. 2021. *Good Practice Principles for Data Ethics in the Public Sector*. https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf

Official Journal of European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Provinsi Jawa Barat. 2020. *Peraturan Gubernur Nomor 13 Tahun 2020 tentang Rencana Induk Sistem Pemerintahan Berbasis Eletronik Pemerintah Daerah Provinsi Jawa Barat Tahun 2019-2023*. Bandung.

Provinsi Jawa Barat. 2021. *Peraturan Daerah Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik, dan Persandian*. Bandung.

UNCTAD. *Data Protection and Privacy Legislation Worldwide*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Yayasan Tifa adalah organisasi yang mempromosikan terwujudnya masyarakat terbuka melalui kerja sama strategis *(strategic partnership)* dengan masyarakat sipil di tingkat lokal, nasional, dan internasional dengan mengedepankan pendekatan pelibatan yang konstruktif *(constructive engagement)*.

Berdiri sejak tahun 2000, Yayasan Tifa telah bekerja bersama dengan lebih dari 700 organisasi mitra yang tersebar di seluruh Indonesia. Dalam kerjanya, Yayasan Tifa mengedepankan dialog dengan masyarakat sipil dan pemangku kebijakan, membangun jaringan dan mengkonsolidasi gerakan, serta mengembangkan kapasitas masyarakat sipil.

Yayasan Tifa konsisten bergerak merespon isu-isu krusial yang mencakup transparansi dan akuntabilitas pemerintah, ekosistem data digital, penguatan demokrasi, keadilan transisional, sumber daya alam, dan pemenuhan hak-hak warga, termasuk di dalamnya hak asasi manusia kelompok rentan dan marjinal.

Yayasan Tifa
18 Office Park Building 15th Fl. Unit C-D
Jl. TB Simatupang No. 18 , RT.2/RW.1, Kebagusan, Pasar Minggu
Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12520
Email: public@tifafoundation.id
Website: www.tifafoundation.id