https://doi.org/10.47548/ijistra.2025.98
Vol. 6, No. 10 , (May, 2025)

Menilai Semula Kedaulatan Data Malaysia:Kritikan Struktural Terhadap Akta Perkongsian Data 2025

Reassessing Malaysia's Data Sovereignty: A Structural Critique of the Data Sharing Act 2025

Qamarul Nazrin Harun

Fakulti Sains Maklumat, Universiti Teknologi MARA, Cawangan Johor, Kampus Segamat, 85000, Malaysia

(qamarulnazrin@uitm.edu.my)

ABSTRAK

Transformasi digital global telah meletakkan data sebagai teras kepada kedaulatan maklumat, kebolehmandirian dasar, dan keutuhan kuasa negara. Dalam konteks ini, Akta Perkongsian Data 2025 (Akta 864) wajar dinilai semula, bukan semata-mata sebagai instrumen pentadbiran data, tetapi sebagai cerminan kesediaan negara mempertahankan kepentingan strategiknya dalam ruang digital. Kajian ini meneliti beberapa kelompongan struktural dalam akta tersebut, termasuk ketiadaan klasifikasi formal terhadap data strategik, ketiadaan prinsip keizinan termaklum yang mantap, serta jurang mekanisme semak dan imbang dalam pelaksanaan kuasa eksekutif. Dengan majoriti penyimpanan data negara masih bergantung kepada infrastruktur asing dan ekosistem digital yang dikawal oleh pihak luar dan berada di luar bidang kuasa nasional, wujud keperluan mendesak untuk memperkukuh prinsip kedaulatan data sebagai asas pembentukan dasar digital negara. Berlandaskan nilai maqasid syariah, amanah institusi, dan prinsip daulat moden, analisis ini mencadangkan pendekatan reformasi yang lebih seimbang antara keperluan keterbukaan dan tuntutan keselamatan maklumat. Pendekatan ini bertujuan membina ekosistem data nasional yang lebih berdaya tahan, berdaulat, dan sejajar dengan aspirasi Malaysia sebagai pemain strategik dalam ekonomi digital serantau.

KATA KUNCI
Kedaulatan Data,
Akta Perkongsian Data 2025,
Kuasa Nasional Digital,
Struktur Tadbir Urus Data,
Maqasid Syariah dalam Dasar Digital.

Received: March 20, 2025 Accepted: May 5, 2025 Published: May 30, 2025

ABSTRACT

The global digital transformation has placed data at the core of information sovereignty, policy sustainability, and the integrity of national power. In this context, the Data Sharing Act 2025 (Act 864) deserves to be re-evaluated, not merely as a data governance instrument, but as a reflection of the country's readiness to defend its strategic interests in the digital space. This study examines several structural gaps in the Act, including the absence of a formal classification of strategic data, the absence of a robust principle of informed consent, and the lack of checks and balances in the exercise of executive power. With the majority of the country's data storage still dependent on foreign infrastructure and externally controlled digital ecosystems beyond national jurisdiction, there is an urgent need to strengthen the principle of data sovereignty as the foundation for national digital policy. Grounded in the values of maqasid syariah, institutional trust, and modern sovereign principles, this analysis proposes a more balanced reform approach between the need for openness and the demands of information security. This approach aims to build a more resilient, sovereign national data ecosystem, aligned with the country's aspirations as a strategic player in the regional digital economy.

KEYWORDS

Data Sovereignty, Data Sharing Act 2025, Digital National Power, Data Governance Structure, Maqasid Shariah in Digital Policy.

1.0 Pengenalan

Dalam era pasca-industri yang dipacu oleh teknologi digital, data telah dianggap sebagai suatu bentuk kuasa baharu yang bukan sahaja menyusun semula ekonomi global, malah telah mengatur semula struktur kuasa antara negara. Jika semasa era kolonialisme fizikal, kuasa dijelmakan melalui penjajahan wilayah dan sumber asli seperti rempah atau minyak, maka abad ke-21 telah menyaksikan data mengambil tempat sebagai "komoditi strategik" yang menentukan siapa yang mengawal naratif, inovasi, dan pengaruh geopolitik (Zuboff, 2019; Couldry & Mejias, 2019). Negara-negara maju seperti Amerika Syarikat dan China berlumba-lumba membina keupayaan pengumpulan, pemprosesan, dan pemilikan data dalam skala besar sebagai senjata diplomasi, ekonomi dan ketenteraan baharu (Floridi, 2020; Wu, 2018). Malah, Kesatuan Eropah secara terbuka menyatakan bahawa kawalan ke atas data ialah sebahagian daripada hak kedaulatan digital mereka, sama seperti kawalan ke atas sempadan fizikal (Pohle & Thiel, 2020).

Namun, kebergantungan global terhadap infrastruktur digital yang dimonopoli oleh segelintir entiti swasta seperti syarikat teknologi gergasi (Big Tech) dari Silicon Valley telah menyebabkan banyak negara kehilangan autonomi terhadap aliran dan pemilikan data warganya sendiri (Hummel, Braun & Dabrock, 2021a). Fenomena ini dikenali sebagai data kolonialisme, iaitu penjajahan bentuk baharu yang tidak lagi menggunakan senjata, tetapi algoritma dan pelayan awan (*cloud server)* (Couldry & Mejias, 2019). Dalam konteks negara membangun, termasuk Malaysia, situasi ini membimbangkan kerana kelemahan infrastruktur tadbir urus data boleh menyebabkan kebocoran maklumat strategik, ketirisan data rakyat, serta eksploitasi oleh pihak luar atas nama transformasi digital (Arun, 2019).

Maka timbul persoalan asas, apakah Malaysia memiliki kerangka undang-undang yang cukup kukuh untuk mempertahankan kedaulatan terhadap data miliknya sendiri? Adakah negara ini sedang berlayar dalam gelombang transformasi digital tanpa sauh kedaulatan yang jelas? Persoalan-persoalan ini membawa kepada perbincangan seterusnya, dengan mencari jawapan kepada apa sebenarnya yang dimaksudkan dengan kedaulatan data, dan mengapa ia harus menjadi asas dalam membentuk kuasa nasional yang berdaulat dan berprinsip?

Dalam erti yang paling asas, kedaulatan data merujuk kepada hak sesebuah negara untuk mengawal, mengurus, dan menentukan bagaimana data di dalam negara digunakan, disimpan, dan dikongsi, selaras dengan nilai dan undang-undang negara tersebut (Floridi, 2020; Pohle & Thiel, 2020; Kuner, 2015a). Namun, konsep ini bukan sekadar isu lokasi *server*) atau pematuhan teknikal, sebaliknya ia menyentuh soal kuasa politik, kendiri digital, dan keupayaan negara untuk menjaga naratif serta identitinya sendiri dalam dunia yang semakin dimonopoli oleh aktor digital luar (Couldry & Mejias, 2019; Hummel, Braun & Dabrock, 2021b; Tisne, 2020; Zuboff, 2019). Isu ini menjadi semakin kritikal apabila infrastruktur digital tempatan masih bergantung kepada vendor asing dan *global cloud ecosystem* yang tertakluk kepada jurisdiksi luar (Arun, 2019; Milan & Treré, 2019; Chenou & Cepeda-Másmela, 2019). Di sinilah pentingnya memahami bagaimana kedaulatan data boleh menjadi asas kepada kuasa nasional, satu persoalan yang akan dibincangkan dengan lebih mendalam dalam seksyen berikutnya.

Walaupun wacana kedaulatan data sering dikaitkan dengan negara-negara maju seperti Kesatuan Eropah, Amerika Syarikat, dan China, realitinya negara-negara membangun seperti Malaysia turut berdepan dengan tekanan yang sama. Di tengah-tengah lonjakan digitalisasi dan ledakan data awam serta peribadi, Malaysia kini berada dalam situasi yang serupa iaitu cuba mengekang risiko penjajahan digital sambil memanfaatkan peluang ekonomi digital (MyDigital, 2021; Milan & Treré, 2019). Namun, berbeza dengan negara berkuasa besar yang memiliki infrastruktur teknologi dan undang-undang yang matang, Malaysia masih bergelut untuk membina kerangka tadbir urus data yang kukuh, terutamanya dari sudut kedaulatan dan keselamatan maklumat strategik. Dalam konteks ini, sebarang dasar atau undang-undang yang menyentuh isu perkongsian dan pemprosesan data bukan sahaja perlu dilihat dari sudut keberkesanan teknokratik semata-mata, tetapi perlu dianalisis secara kritikal dari lensa kuasa, hak, dan kendiri negara terhadap ruang digitalnya sendiri. Maka tidak menghairankan apabila Akta Perkongsian Data 2025 (Akta 864) muncul sebagai salah satu instrumen terpenting dalam pergelutan ini.

Dalam arus deras pembangunan digital Malaysia, isu kedaulatan data bukan sekadar wacana pinggiran, ia merupakan komponen asas yang menentukan keberdayaan digital negara secara menyeluruh. Rangka strategi seperti *Malaysia Digital Economy Blueprint* (MyDigital, 2021) dan Pelan Induk Perindustrian Baharu 2030 (NIMP 2030) secara konsisten menekankan penggunaan data raya (*big data*), kecerdasan buatan (AI), dan automasi sebagai pemacu utama daya saing nasional. Namun, pembangunan ini bergantung

sepenuhnya kepada keupayaan negara untuk mengakses, melindungi, dan mengawal data rakyat serta sistem maklumat awam secara berdaulat. Tanpa kedaulatan data, transformasi digital akan mudah terjerumus ke dalam jerat ketergantungan teknologi luar, manipulasi algoritma tanpa kawalan, dan pencerobohan privasi yang menjejaskan kepercayaan awam (Floridi, 2020; Zuboff, 2019; Pohle & Thiel, 2020). Lebih membimbangkan, jika negara gagal menentukan sempadan kendiri dalam mengurus data strategik, maka naratif pembangunan itu sendiri berisiko ditentukan oleh pihak luar yang memiliki keupayaan teknikal dan akses analitik yang lebih unggul. Maka, dalam mendepani revolusi industri 4.0 dan ekonomi data masa hadapan, kedaulatan data harus dilihat bukan sebagai pilihan tambahan, tetapi sebagai syarat mutlak untuk memastikan kemerdekaan digital negara kekal terpelihara.

Sebagai sebahagian daripada agenda mempercepatkan transformasi digital dan merealisasikan aspirasi Malaysia sebagai hab data serantau, Kerajaan telah memperkenalkan Akta 864. Akta ini dilihat sebagai inisiatif perundangan pertama yang menyusun secara sistematik proses perkongsian data antara agensi kerajaan, yang sebelum ini beroperasi secara terasing (*silo-based*) dan tidak seragam (MAMPU, 2022). Matlamat utamanya adalah untuk membolehkan data awam dimanfaatkan dengan lebih cekap dalam pembuatan dasar, peningkatan mutu perkhidmatan awam, serta pemerkasaan sistem penyampaian berasaskan data raya dan kecerdasan buatan (MyDigital, 2021). Akta ini juga memperkenalkan struktur pelaksanaan tersendiri seperti penubuhan Jawatankuasa Perkongsian Data Negara (Seksyen 5), pelantikan Ketua Pengarah Jabatan Digital Negara (Seksyen 11), serta prosedur formal bagi permintaan dan pengurusan data (Seksyen 12). Pada permukaannya, Akta 864 ini tampak seiring dengan tuntutan modenisasi pentadbiran digital negara. Namun begitu, soal pokoknya masih kekal iaitu adakah akta ini benar-benar kukuh untuk memelihara prinsip kedaulatan data, atau sekadar melicinkan aliran data tanpa perlindungan terhadap kuasa dan hak digital negara?

Berdasarkan latar global yang memperlihatkan bagaimana data telah menjadi teras kuasa strategik abad ini, serta keperluan mendesak Malaysia untuk mempertahankan kendiri digitalnya di tengah-tengah lonjakan pembangunan ekonomi data, kedaulatan data muncul sebagai isu yang tidak boleh dielakkan. Akta 864 dilihat sebagai usaha kerajaan untuk merasionalisasi ekosistem data sektor awam, namun masih menimbulkan persoalan kritikal berkenaan sejauh mana ia memperkukuh atau melemahkan keupayaan negara dalam mengawal, melindungi, dan menentukan nasib datanya sendiri. Maka, artikel ini bertujuan untuk menilai secara kritikal struktur dan kandungan Akta 864 dari sudut kedaulatan data, serta menganalisis implikasi undang-undang ini terhadap kuasa nasional Malaysia dalam era digital. Perbincangan ini diharap dapat menyumbang kepada wacana dasar yang lebih holistik dan berpaksikan prinsip kedaulatan maklumat sebagai tiang utama keadilan digital dan kemerdekaan negara.

2.0 Memahami Kedaulatan Data sebagai Landasan Strategik Kuasa Nasional

Kedaulatan tidak pernah bersifat neutral. Ia adalah penentu siapa yang layak memimpin, siapa yang berhak menentukan arah, dan siapa yang diberi kepercayaan untuk menjaga sesuatu yang lebih besar daripada dirinya. Dalam konteks negara, data bukan sekadar alat pentadbiran atau bahan mentah analitik, bahkan ia adalah wajah moden kepada kuasa yakni kuasa untuk memahami, mempengaruhi, dan mengarah realiti. Oleh itu, kedaulatan data tidak boleh dipisahkan daripada asas daulat yang memberi legitimasi kepada kuasa. Ia mesti ditakrif bukan hanya melalui sempadan hukum atau keupayaan teknikal, tetapi melalui prinsip amanah, keadilan dan kebertanggungjawaban.

2.1 Daulat sebagai asas legitimasi kuasa

Konsep daulat dalam tradisi politik Melayu-Islam bukan sekadar warisan simbolik atau adat pertabalan raja. Ia merujuk kepada legitimasi kuasa yang bersifat sakral, iaitu suatu bentuk keabsahan yang lahir daripada anugerah Ilahi kepada pemimpin yang diberi amanah untuk mentadbir dengan adil, beradab dan penuh hikmah (Milner, 2002; Syed Muhammad Naquib al-Attas, 1978). Dalam kerangka ini, daulat bukan ditentukan oleh pemilikan kekuatan ketenteraan, kekayaan atau undang-undang semata-mata, tetapi berdasarkan tanggungjawab moral dan akhlak kepimpinan terhadap kesejahteraan umat. Ia adalah kuasa yang sah kerana ia berfungsi menjaga manusia, bukan menguasai mereka.

Jika ditinjau dari perspektif teologi Islam, kedaulatan tidak terikat pada sempadan negara-bangsa moden. Ia bersifat transnasional, merentasi geografi dan sistem kenegaraan kontemporari. Dalam Islam, hanya Allah SWT yang memiliki kedaulatan mutlak (al-hakimiyyah), dan manusia sebagai khalifah diberi amanah untuk mentadbir bumi atas prinsip keadilan dan syura (Qur'an, al-Baqarah 2:30; al-Nisa' 4:58). Maka,

sebarang bentuk kuasa politik, termasuklah kawalan ke atas data dan maklumat dalam dunia moden mestilah tunduk kepada prinsip-prinsip maqasid syariah, iaitu menjaga agama, nyawa, akal, keturunan dan harta (Auda, 2008). Dalam konteks ini, daulat bukan hak, tetapi amanah; bukan dominasi, tetapi perkhidmatan kepada Ummah.

Perlu ditegaskan bahawa dalam zaman digital, bentuk kuasa telah berubah. Jika dahulu sempadan fizikal, wilayah, dan kedaulatan raja menjadi simbol kekuasaan, hari ini data menjadi medan baru tempat kuasa ditentukan (Zuboff, 2019; Couldry & Mejias, 2019). Namun prinsip daulat tidak berubah. Kedaulatan era maklumat masih perlu diasaskan atas keadilan, keterbukaan, dan perlindungan terhadap makhluk, bukan eksploitasi. Maka, sebarang bentuk pengumpulan, pemprosesan, atau perkongsian data oleh negara atau entiti korporat tidak boleh dilakukan atas nama efisiensi semata-mata. Ia perlu dilakukan atas nama legitimasi yang sah, iaitu daulat yang memelihara hak dan maruah manusia.

Dalam konteks 'Ummah', kelemahan kedaulatan data telah mendedahkan dunia Islam kepada pelbagai bentuk kolonialisme digital. Negara-negara Muslim menjadi pengguna pasif teknologi asing, platform sosial global, dan infrastruktur awan yang dikawal oleh kuasa luar. Tanpa kerangka kuasa yang sah dan berdaulat dalam dunia digital, Ummah berisiko kehilangan naratif, memori kolektif, dan bahkan arah tuju sosial-politik sendiri (Elasha, 2021; Sardar, 2003). Oleh itu, pembangunan kuasa digital yang berdaulat dan beradab adalah suatu keperluan bukan sahaja untuk mempertahankan kemerdekaan negara, tetapi juga untuk memulihkan maruah peradaban Islam yang kini bergerak dalam lanskap siber yang tidak seimbang.

Dengan ini, pemahaman tentang daulat mesti diperluas dari takrifan klasik kepada dimensi baru yang sejajar dengan realiti digital. Daulat digital mestilah diasaskan bukan sekadar pada kuasa teknokratik, tetapi atas prinsip adil, amanah, dan legitimasi moral dalam mengurus data sebagai amanah besar terhadap rakyat dan Ummah seluruhnya.

2.2 Data sebagai aset, amanah dan naratif bangsa

Jika dalam dunia fizikal, negara mempertahankan tanah, sumber asli, dan perairannya sebagai aset strategik, maka dalam dunia digital, data telah mengambil tempat yang setara; Malah dalam banyak hal, lebih sensitif dan rentan. Data bukan lagi dianggap sebagai maklumat mentah semata-mata; ia adalah aset negara, modal kuasa, dan lebih mendalam lagi, naratif tentang siapa kita (Zuboff, 2019; Floridi, 2020). Ia mengandungi gambaran bukan hanya tentang tingkah laku rakyat, tetapi juga sejarah, cita rasa, ketakutan, dan harapan mereka. Dalam tangan yang salah, data boleh digunakan untuk membentuk persepsi, memanipulasi masyarakat, atau mengalihkan hala tuju dasar negara tanpa pengetahuan rakyat sendiri (Couldry & Mejias, 2019).

Namun, data bukan hanya tentang kuasa, ia juga amanah. Dalam pandangan etika Islam, setiap bentuk maklumat yang berkait dengan manusia adalah sebahagian daripada hak insan yang perlu dijaga, bukan dimanipulasi (Auda, 2008). Apabila negara mengumpul data rakyat, sama ada tentang lokasi, kesihatan, aktiviti digital, atau hubungan sosial; Ia sedang mengambil tanggungjawab besar untuk melindungi maruah individu dan kolektif bangsa. Amanah ini bukan sekadar terhadap rakyat, tetapi juga terhadap Allah SWT sebagai pemilik mutlak segala ilmu dan maklumat (al-Baqarah, 2:255). Maka, tindakan menyimpan, memproses, dan berkongsi data harus tunduk kepada prinsip keadilan, kejelasan niat, dan perlindungan daripada penyalahgunaan, bukan sekadar pematuhan peraturan prosedural.

Lebih daripada itu, data adalah naratif bangsa. Dalam kerangka inilah data membentuk sejarah kolektif, maklumat tentang identiti budaya, bahasa, adat tempatan, serta pola sosial yang membentuk keperibadian sesebuah negara. Siapa yang memiliki data, dialah yang berupaya menulis dan mengawal naratif. Tanpa kawalan terhadap data sendiri, bangsa itu berisiko kehilangan kebebasan menentukan sejarah dan masa depannya (Pohle & Thiel, 2020; Hummel et al., 2021b). Maka kedaulatan ke atas data menjadi keperluan bukan hanya untuk keselamatan, tetapi juga untuk kelangsungan identiti dan suara.

Pengurusan data tidak seharusnya dimonopoli oleh kerajaan pusat atau syarikat korporat, tetapi perlu melibatkan peranan komuniti akar umbi seperti masjid, kampung, NGO, institusi agama dan Pendidikan sebagai penjaga data mikro yang memahami konteks lokal. Pendekatan ini lebih selari dengan prinsip Islam yang menekankan keadilan yang bersifat setempat ('adalah mahalliyyah) dan kebertanggungjawaban sosial yang dikongsi (Ibn Khaldun, 1967). Melalui pendekatan ini, data menjadi sesuatu yang dimuliakan, bukan semata-mata ditadbir atau dieksploitasi.

Justeru, untuk sebuah negara mengekalkan maruah dan kekuatan naratifnya, ia mesti melihat data bukan hanya sebagai alat, tetapi sebagai warisan kolektif yang wajib dijaga dengan penuh adab, hikmah, dan rasa takut kepada amanah.

2.3 Kedaulatan data: Daulat digital dalam era maklumat

Dalam era maklumat yang semakin mendefinisikan kuasa negara dan masa depan umat manusia, istilah kedaulatan data telah menjadi medan pertarungan baharu antara kepentingan nasional, entiti korporat transnasional, dan hak individu. Dalam kerangka barat, "*data sovereignty*" sering didefinisikan sebagai hak negara untuk memastikan data warganya tertakluk kepada undang-undang dan jurisdiksi domestik, terutama dari sudut lokasi fizikal penyimpanan dan kawalan data (Kuner, 2015a; Pohle & Thiel, 2020). Ia berpaksikan model Westphalia iaitu negara berdaulat yang menetapkan sempadan hukum atas wilayah dan aset maklumatnya (Floridi, 2020; Berlin, 2018). Namun, pemahaman ini terlalu sempit jika melihat data sekadar sebagai "aset negara", bukan sebagai amanah terhadap manusia dan Tuhan.

Kedaulatan bukan sekadar soal kawalan, tetapi soal siapa yang layak memimpin maklumat dengan adil, bermaruah, dan beradab. Dalam dunia yang dibanjiri oleh aliran data tanpa sempadan, daulat digital hanya sah jika diasaskan atas prinsip maqasid (Auda, 2008; al-Raysuni, 2006). Data ialah manifestasi baru kepada semua ini kerana ia boleh digunakan untuk melindungi atau menghancurkan akal, maruah, dan keselamatan umat. Maka, kedaulatan data yang tidak diasaskan atas niat menjaga makhluk dan memelihara kebenaran adalah kuasa tanpa ruh.

Tambahan pula, pendekatan teknokratik semata-mata seperti yang digariskan dalam Data Governance Acts di EU atau US CLOUD Act, cenderung menyamakan kedaulatan dengan kawalan unilateral oleh negara atau entiti digital besar (Bradford, 2020; Greenleaf, 2019). Namun, ini menimbulkan paradoks baru iaitu negara menjadi pelindung data rakyat, tetapi dalam masa yang sama, berpotensi menjadi pemantau mutlak yang mengancam privasi dan kebebasan warganya sendiri (Morozov, 2011; Zuboff, 2019). Dalam konteks ini, apa yang diperlukan bukan hanya "kuasa negara atas data", tetapi kuasa yang sah secara moral, seperti yang diungkap oleh al-Ghazali, bahawa kekuasaan tanpa keadilan ialah kerosakan yang lebih dahsyat daripada kekacauan itu sendiri (al-Ghazali, 1985).

Kedaulatan data yang berpaksikan daulat menuntut bahawa negara tidak boleh menjadi pemilik mutlak data, sebaliknya menjadi penjaga amanah maklumat, dan memposisikan dirinya sebagai murabbi digital yang mentadbir dengan hikmah, bukan sebagai penguasa algoritma (Mokhtar, 2022). Ini penting kerana dalam dunia algoritma hari ini, maklumat boleh membentuk realiti. Ia boleh menaikkan pemimpin, membentuk ketakutan massa, memecah-belah masyarakat, atau menghapuskan sejarah dan memori kolektif. Tanpa daulat digital yang adil, maklumat menjadi senjata bukan hanya dalam konflik antarabangsa, tetapi juga dalam bentuk penjajahan epistemologi di mana wacana, suara, dan nilai tempatan diketepikan oleh naratif luar yang disalurkan melalui data yang tidak dikawal (Sardar, 1998; Milan & Treré, 2019).

Bahkan lebih membimbangkan, umat Islam hari ini menyumbang secara aktif kepada ekosistem digital global, tetapi tidak memiliki kawalan bermakna terhadap data, teknologi, mahupun piawaian nilai dalam ruang siber. Hasilnya, wacana Islam sering disaring melalui lensa algoritma luar yang tidak memahami konteks, bahasa, atau sensitiviti nilai (Elasha, 2021; Yaacob, 2023). Justeru, kedaulatan data mesti difahami bukan sekadar sebagai keupayaan teknikal negara, tetapi sebagai syarat untuk mempertahankan kebebasan Ummah daripada penjajahan digital yang terancang. Ia adalah suatu tanggungjawab kolektif untuk mewujudkan sistem data yang berpaksikan rahmah, keadilan, dan maruah insan.

2.4 Kedaulatan data sebagai infrastruktur kuasa strategik

Tidak semua negara yang memiliki data mampu membina kuasa. Yang membezakan kuasa digital yang mandiri daripada ketergantungan adalah satu perkara: infrastruktur. Kedaulatan data yang sebenar tidak terletak pada kenyataan dasar atau akta semata, tetapi pada keupayaan fizikal dan teknikal negara untuk menyimpan, melindungi dan mengendalikan datanya sendiri. Dalam konteks ini, kedaulatan data bukan hanya prinsip normatif, tetapi struktur kuasa yang bergantung kepada logistik digital, kejuruteraan awan, dan keupayaan kendiri terhadap maklumat (Chander & Le, 2014; Kuner, 2015a).

Bagi Malaysia, kebanyakan sistem data awam termasuk rekod kesihatan, pendidikan, dan keselamatan sosial masih bergantung kepada penyedia infrastruktur luar negara. Ketergantungan ini bukan sekadar soal

kos, tetapi mewujudkan risiko strategik iaitu data rakyat disimpan di luar sempadan jurisdiksi, dikendalikan oleh pihak yang mungkin tertakluk kepada undang-undang asing, serta rentan terhadap penyalahgunaan, manipulasi, atau pencerobohan siber (Bradford, 2020; Klimburg, 2017). Lebih berbahaya, dalam situasi ketegangan geopolitik atau konflik siber, data ini boleh dijadikan senjata tekanan, termasuk dalam bentuk pembekuan akses, pemantauan rahsia, atau gangguan sistem kritikal negara (UNCTAD, 2021; OECD, 2022).

Kedaulatan data sebagai infrastruktur kuasa menuntut agar negara memiliki pelayan fizikal (*on-soil servers*), sistem penyimpanan awan berasaskan lokal (sovereign cloud), protokol keselamatan end-to-end yang dibangunkan secara nasional, serta kawalan penuh ke atas proses penyimpanan, pengesanan, dan pemprosesan data. Tanpa komponen ini, negara hanya mempunyai ilusi kawalan; sedangkan data sebagai "darah" kepada sistem digital, mengalir melalui saluran yang tidak diketahui, dimiliki oleh entiti luar yang tidak tertakluk kepada nilai atau undang-undang negara tersebut (Floridi, 2020; Taddeo & Floridi, 2018).

Di sinilah pentingnya melihat pembangunan infrastruktur data bukan sebagai inisiatif IT semata-mata, tetapi sebagai benteng kedaulatan moden. Negara-negara seperti China dan Jerman telah pun melaksanakan model data localization yang ketat, membina pusat data nasional mereka sendiri, serta mengawal trafik maklumat strategik melalui infrastruktur milik negara (Greenleaf, 2019; MyDigital, 2021). Dalam kes China, kawalan ini bukan sahaja soal keselamatan, tetapi juga memberi kelebihan ekonomi kerana mereka memiliki ekosistem data yang tersendiri yang membolehkan pembangunan AI tempatan, dasar fiskal berdasarkan data real-time, serta jaringan perdagangan digital yang berautonomi (Zeng, Stevens & Chen, 2021).

Tanpa kemampuan yang setara, negara-negara membangun akan terus menjadi koloni maklumat, bergantung kepada teknologi luar bukan sahaja untuk beroperasi, tetapi untuk memahami rakyatnya sendiri. Lebih parah, negara mungkin menyusun dasar berdasarkan data yang diperoleh melalui sistem luar yang tidak telus dan tidak boleh diaudit (Souter, 2020; Milan & Treré, 2019). Ini bukan hanya melemahkan keupayaan dasar, tetapi membentuk "dependency trap" yang menyukarkan kebangkitan digital berasaskan kendiri dan nilai lokal.

Malaysia mesti membina infrastruktur data berdaulat sebagai sebahagian daripada pertahanan negara. Dalam dunia di mana kuasa tidak lagi dihitung melalui sempadan fizikal semata-mata, tetapi melalui kawalan maklumat, "sovereign data infrastructure" ialah pangkalan kuasa keempat negara, setanding dengan darat, laut, dan udara (Klimburg, 2017). Ini termasuk pelaburan dalam kemudahan fizikal (pusat data tempatan), sumber manusia berkemahiran tinggi, pelaksanaan piawaian keselamatan siber nasional, serta ekosistem perundangan yang memastikan segala data strategik kekal dalam kawalan nasional, meskipun dalam sistem *cloud* atau perkongsian antarabangsa.

Ringkasnya, kedaulatan tidak akan wujud tanpa asas fizikal untuk menampungnya. Negara yang ingin bebas dalam membuat keputusan, menyusun naratif, dan melindungi rakyatnya, perlu bermula dengan memiliki infrastruktur maklumatnya sendiri. Tanpa ini, setiap dasar, setiap strategi, dan setiap visi digital negara adalah bayangan yang bersandar pada pelantar milik orang lain.

2.5 Antara kedaulatan, ketelusan dan hak rakyat

Kedaulatan data, jika tidak ditimbang dengan cermat, boleh dengan mudah tergelincir menjadi bentuk baharu autoritarianisme digital, di mana atas nama kuasa dan keselamatan, negara bertindak sebagai pemilik mutlak maklumat rakyatnya. Namun, dalam kerangka daulat yang sah, kuasa tidak berdiri sendiri. Ia terikat pada nilai amanah, keadilan, dan keterbukaan, serta harus disemak oleh suara dan hak rakyat sebagai pemegang asal maklumat tersebut (Auda, 2008; al-Ghazali, 1985). Maka, cabaran utama kedaulatan data hari ini bukan sekadar membina kuasa ke atas data, tetapi menjaganya tanpa mengkhianati kepercayaan yang datang bersama maklumat itu.

Dalam banyak sistem perundangan dan polisi digital dunia, prinsip "*informed consent*", "*data minimisation*", dan "*transparency by design*" telah menjadi asas kepada tadbir urus data yang adil dan lestari (GDPR, 2018; OECD, 2022). Namun, pendekatan ini sering dilaksanakan secara simbolik, sekadar memenuhi keperluan undang-undang tanpa memperkukuh keterlibatan rakyat. Hakikatnya, ketelusan dalam pengurusan data awam bukan hanya soal memaparkan polisi privasi atau memberi borang kebenaran. Ia menuntut sistem pengurusan data yang memberi ruang kepada rakyat untuk mengetahui, menyoal, dan menolak penggunaan maklumat mereka dalam konteks yang tidak mereka persetujui (Tisne, 2020; Zuboff, 2019).

Lebih penting, dalam konteks negara-negara membangun seperti Malaysia yang masih berada dalam fasa konsolidasi transformasi digital, ketelusan dan kepercayaan rakyat bukan sekadar nilai tambahan, tetapi syarat kepada keberkesanan dasar digital itu sendiri. Tanpa kepercayaan, rakyat akan menolak untuk mendaftar, berkongsi, atau menyertai ekosistem digital negara, lalu membuka ruang kepada penggunaan sistem tidak rasmi, platform asing, dan akhirnya menghakis legitimasi negara sendiri dalam ruang digital (Floridi, 2020; Morozov, 2011).

Di sinilah pentingnya meletakkan etika sebagai teras kepada kedaulatan. Negara perlu merangka semula kerangka kuasa digitalnya dengan mengakui bahawa rakyat ialah pemilik asal data, bukan sekadar subjek maklumat. Ini bermakna mesti wujud sistem “opt-out” untuk penggunaan tidak kritikal, notifikasi awam bagi semua pemindahan data strategik, mekanisma aduan dan semakan, serta laporan awam tahunan tentang penggunaan data oleh agensi kerajaan dan rakan teknologinya. Kedaulatan tidak akan sah tanpa ketelusan, dan ketelusan tidak bermakna tanpa kebertanggungjawaban.

Tambahan pula, dari perspektif Islam, prinsip mas’uliyyah (pertanggungjawaban) menggariskan bahawa setiap bentuk kuasa adalah ujian, dan setiap maklumat yang dipegang adalah beban yang akan disoal di akhirat. Maka, pengurusan data rakyat bukan hanya persoalan teknokratik atau polisi digital tetapi amanah syarie yang perlu dipikul dengan rasa takut, rendah diri dan tanggungjawab spiritual (al-Raysuni, 2006; Syed Muhammad Naquib al-Attas, 1978).

Akhirnya, kedaulatan data yang tidak berakar pada kepercayaan akan gagal membina legitimasi, dan negara yang tidak telus akan kehilangan naratifnya sendiri. Dalam era di mana maklumat lebih pantas daripada penguatkuasaan, daulat digital hanya akan hidup jika ia ditopang oleh hikmah, keterbukaan, dan keberanian untuk menjawab kepada rakyat.

3.0 Gambaran Umum Akta Perkongsian Data 2025

Akta 864 merupakan inisiatif legislatif pertama di Malaysia yang memperincikan kerangka perundangan khusus bagi mengawal selia perkongsian data antara agensi sektor awam. Akta ini digubal atas dasar keperluan untuk menyusun semula ekosistem maklumat kerajaan yang selama ini bersifat silo, tidak saling beroperasi (interoperable), serta bergantung kepada budi bicara dan kesediaan manual antara jabatan. Ia secara rasmi telah diluluskan di Parlimen pada Disember 2024 dan diwartakan pada 20 Februari 2025.

Dari sudut struktur, Akta ini merangkumi lima bahagian utama dan 29 seksyen. Inti utama akta ini adalah untuk menyediakan rangka kawal selia formal bagi proses permintaan, pertimbangan, dan perkongsian data antara agensi persekutuan, termasuk melalui pelantikan Jawatankuasa Perkongsian Data Negara (Seksyen 5) dan Ketua Pengarah Jabatan Digital Negara (Seksyen 11) sebagai pelaksana utama. Proses ini melibatkan permintaan rasmi (Seksyen 12), justifikasi tujuan (Seksyen 13), semakan keselamatan (Seksyen 14), hak untuk menolak (Seksyen 15), serta kewajipan teknikal dan rekod yang mesti dipatuhi (Seksyen 16–18).

Antara elemen yang membezakan Akta ini ialah keupayaannya memperkenalkan rukun perkongsian data tersendiri (Seksyen 4), memperincikan definisi agensi awam dan struktur permintaan, serta menyediakan saluran formalisasi data terbuka (Seksyen 20). Ia turut membenarkan pengecualian pelaksanaan atas budi bicara menteri (Seksyen 27), serta memberikan perlindungan undang-undang kepada pegawai pelaksana kerajaan daripada tindakan guaman dalam menjalankan tugas (Seksyen 24), suatu ciri yang menandakan keinginan untuk mengukuhkan kuasa negara dalam pengurusan maklumat strategik.

Dari segi latar penggubalan, Akta ini lahir daripada proses perundangan yang melibatkan kajian komparatif dengan tujuh negara luar, termasuk EU, UK, Australia dan Singapura, serta lebih 140 sesi libat urus dengan kementerian, agensi negeri, sektor swasta dan badan berkanun dari 2023 hingga 2024. Ini menunjukkan bahawa Akta ini bukan sahaja dibina dari sudut keperluan domestik, tetapi juga beraspirasi untuk menepati piawaian global dalam tadbir urus data kerajaan. Secara keseluruhan, Akta 864 disusun dengan objektif untuk:

1. Menjadikan proses perkongsian data lebih sistematik, telus dan terjamin, terutamanya dalam perkhidmatan awam;

2. Mempercepatkan dasar berasaskan data, sejajar dengan hala tuju transformasi digital negara di bawah MyDigital;
3. Menggalakkan keterbukaan dan kerjasama maklumat antara jabatan, sambil mengawal aspek keselamatan dan privasi.

Namun begitu, meskipun Akta ini tampak menyeluruh dari segi struktur teknikal dan prosedural, beberapa seksyen kritikal seperti kuasa pengecualian (Seksyen 27), ketiadaan prinsip kebenaran bermaklumat, serta ketidakjelasan tentang klasifikasi data strategik negara telah menimbulkan persoalan sama ada kerangka ini benar-benar dapat mempertahankan kedaulatan data negara dalam erti sebenar, atau sekadar mempermudah aliran data tanpa benteng kawalan yang cukup.

Oleh itu, perbahasan seterusnya dalam artikel ini akan menganalisis kelemahan struktur Akta 864 dari sudut prinsip kedaulatan data, dan sejauh mana ia membantu atau menjejaskan keupayaan Malaysia dalam membina kuasa digital berdaulat.

4.0 Analisa Struktural terhadap Kelemahan Akta dari Sudut Kedaulatan Data

Meskipun Akta 864 disusun dengan matlamat untuk memperkukuh tadbir urus data antara agensi kerajaan, pembacaan teliti terhadap struktur dan peruntukannya mendedahkan beberapa kekosongan kritikal yang boleh melemahkan kedudukan Malaysia dalam mempertahankan kedaulatan datanya. Akta ini, secara teknikal, bersifat prosedural dan birokratik, ia memberi penekanan kepada aliran data yang efisien, tetapi kurang memberi penekanan kepada dimensi strategik, moral dan geopolitik data sebagai kuasa nasional.

Kritikan utama yang timbul ialah bahawa Akta ini memperkemas sistem perkongsian data, tetapi tidak memperkukuh tembok kawalan yang membezakan antara penggunaan beretika dengan eksploitasi maklumat. Ia membentuk saluran formal, tetapi tidak menetapkan pagar nilai. Akibatnya, beberapa seksyen utama dalam akta ini membuka ruang besar kepada penyalahgunaan kuasa, manipulasi tujuan, dan ketirisan maklumat strategik tanpa mekanisma semak dan imbang yang berkesan.

Lebih membimbangkan, akta ini belum menunjukkan kejelasan terhadap makna kedaulatan data dalam konteks negara membangun. Prinsip-prinsip penting seperti kebenaran bermaklumat, pengawalan infrastruktur digital, dan klasifikasi aset strategik masih belum diangkat secara tuntas sebagai tonggak perlindungan dalam struktur perundangan sedia ada.

Sehubungan itu, bahagian ini akan menganalisis secara struktural enam kelemahan utama yang dapat dikenalpasti dalam Akta 864, berdasarkan prinsip kedaulatan data yang telah dihuraikan dalam seksyen sebelumnya. Setiap kelemahan akan dibincangkan dari sudut teks perundangan, implikasi praktikal, serta risiko kepada kuasa nasional dan kepercayaan rakyat.

4.1 Takrifan tujuan sah yang terlalu umum dan longgar

Salah satu asas utama kepada sebarang bentuk perkongsian data ialah tujuan penggunaannya. Dalam Akta 864, persoalan ini disentuh dalam Seksyen 13, yang memperincikan justifikasi permintaan data antara agensi. Namun, perenggan terakhir dalam seksyen tersebut menimbulkan kebimbangan besar apabila ia menyatakan bahawa data boleh dikongsi untuk “apa-apa tujuan lain sebagaimana yang boleh ditentukan oleh Jawatankuasa.”

Pada zahirnya, klausa ini memberikan fleksibiliti kepada Jawatankuasa Perkongsian Data Negara untuk menilai permintaan berdasarkan konteks dan keperluan semasa. Namun, dari sudut kedaulatan data, ketidakjelasan frasa tersebut memperlihatkan kelemahan asas dalam menghadkan skop kuasa. Frasa seperti “apa-apa tujuan” tanpa sempadan substantif membuka ruang kepada tafsiran bebas, yang dalam situasi tertentu boleh disalah guna untuk memenuhi kehendak politik, tekanan luar, atau kepentingan pihak berkepentingan yang tidak semestinya selaras dengan kepentingan nasional (Greenleaf, 2019; Hummel et al., 2021a).

Daripada perspektif perundangan data antarabangsa, undang-undang yang kukuh biasanya menetapkan tujuan terhad dan boleh diaudit, seperti yang diamalkan dalam General Data Protection Regulation (GDPR) Kesatuan Eropah, di mana setiap permintaan mestilah “specific”, “explicit”, dan “legitimate” (GDPR, 2018). Ketidaktepatan dalam mendefinisikan ‘tujuan’ bukan sahaja membuka ruang penyalahgunaan, tetapi juga

menghakis prinsip “purpose limitation”, yang menjadi asas kepada kebolehpercayaan sistem maklumat kerajaan (Tisne, 2020).

Memberikan kuasa sebegitu luas tanpa mekanisma semakan berkala atau had prinsipil boleh mewujudkan ketidakseimbangan kuasa maklumat, di mana data rakyat beralih tangan antara agensi tanpa garis panduan nilai yang jelas. Lebih membimbangkan, proses penentuan “tujuan lain” itu dilakukan oleh Jawatankuasa yang tidak tertakluk kepada ketelusan awam, semakan parlimen, atau keperluan penerbitan rasional secara terbuka.

Oleh itu, kelemahan pada Seksyen 13(e) bukan sekadar isu teks, tetapi mencerminkan kekosongan struktur dalam memastikan prinsip daulat digital dihormati. Negara yang berdaulat tidak boleh memberi kuasa interpretasi maklumat tanpa sempadan substantif, kerana maklumat bukan sekadar aset teknikal, tetapi merupakan suatu bentuk amanah dan kuasa yang perlu ditadbir dengan batas yang tegas, bukan kelonggaran yang luas.

4.2 Ketiadaan prinsip kebenaran bermaklumat (Informed consent)

Prinsip kebenaran bermaklumat atau informed consent merupakan hak individu untuk mengetahui bila dan mengapa datanya digunakan, serta untuk memberikan atau menarik semula persetujuan. Dalam Akta 864, prinsip ini tidak dinyatakan secara eksplisit atau tersirat, bahkan tidak disentuh walaupun secara prinsipil dalam mana-mana seksyen. Ini menimbulkan satu kelompongan serius dari sudut pengiktirafan hak rakyat terhadap maklumat peribadi mereka sendiri.

Menurut peruntukan akta, data peribadi yang dimiliki oleh satu agensi kerajaan boleh dikongsi dengan agensi lain atas permintaan rasmi yang diluluskan oleh Jawatankuasa (Seksyen 12–15), tanpa keperluan untuk memaklumkan pemilik data atau mendapatkan kebenaran mereka terlebih dahulu. Walaupun pendekatan ini mungkin wajar dalam konteks keselamatan nasional atau perkhidmatan kecemasan, penggunaan prinsip yang sama untuk semua kategori data dan semua tujuan boleh mengakibatkan kehilangan asas kepercayaan awam terhadap ekosistem digital negara.

Dalam banyak undang-undang perlindungan data antarabangsa, termasuk GDPR dan APEC Privacy Framework, informed consent bukan hanya menjadi standard, tetapi teras legitimasi kepada pemprosesan data peribadi (GDPR, 2018; APEC, 2015). Tanpa persetujuan atau sekurang-kurangnya notifikasi, pemilik data dinafikan hak mereka untuk mengetahui bagaimana, bila, dan untuk tujuan apa data mereka dikongsi, sekali gus mengurangkan mereka kepada objek statistik yang pasif, bukan subjek hak yang aktif (Zuboff, 2019).

Pemilikan maklumat berkaitan seseorang individu adalah sebahagian daripada maruah (karamah insaniyyah) yang perlu dijaga. Apabila negara bertindak atas nama rakyat, ia mesti dilakukan dengan amanah, dan amanah tidak wujud tanpa keterbukaan. Maka, kedaulatan data yang tidak disertai mekanisma pemberitahuan dan kebenaran rakyat akan dilihat sebagai kedaulatan yang tidak berdaulat secara moral kerana ia tidak berpijak pada prinsip adil terhadap makhluk (Auda, 2008; al-Raysuni, 2006).

Ketiadaan sistem notifikasi, borang kebenaran, atau hak untuk opt-out bagi penggunaan data yang tidak melibatkan keselamatan atau darurat menunjukkan bahawa akta ini cenderung melihat data sebagai aset agensi, bukan amanah rakyat. Ini bertentangan dengan aspirasi Malaysia untuk membina ekonomi digital berasaskan kepercayaan, seperti yang terkandung dalam dokumen MyDigital (MyDigital, 2021).

Oleh itu, kelemahan Akta 864 dalam mengiktiraf prinsip kebenaran bermaklumat bukan hanya isu teknikal, tetapi cabaran moral terhadap legitimasi negara dalam ruang digital. Untuk menjadi negara yang berdaulat dalam maklumat, rakyat mesti dilibatkan bukan hanya sebagai objek data, tetapi sebagai pemegang taruh dalam bagaimana maklumat mereka digunakan dan dikongsi. Rakyat berhak untuk mengetahui, bersetuju atau menolak bagaimana data mereka digunakan.

4.3 Kuasa pengecualian menteri yang tidak disekat

Salah satu peruntukan paling kontroversial dalam Akta 864 ialah Seksyen 27, yang menyatakan bahawa: “Menteri boleh, melalui perintah yang disiarkan dalam warta, tertakluk kepada apa-apa syarat atau sekatan yang difikirkannya perlu atau suai manfaat untuk dikenakan, mengecualikan mana-mana orang atau

golongan orang daripada mana-mana atau semua peruntukan akta ini." Walaupun secara teknikal ia berbentuk pengecualian yang perlu diwartakan, peruntukan ini memberikan kuasa unilateral kepada menteri untuk mengabaikan keseluruhan struktur kawal selia yang digubal dalam akta ini tanpa keperluan semakan Parlimen, konsultasi awam, atau penilaian bebas.

Dari sudut prinsip pentadbiran moden, peruntukan seperti ini menimbulkan persoalan besar tentang ketelusan, kebertanggungjawaban, dan sempadan kuasa eksekutif. Dalam konteks kedaulatan data, kuasa pengecualian yang tidak terhad bukan sahaja melemahkan prinsip tadbir urus, tetapi juga mewujudkan kekaburan dalam pengurusan data strategik, yang boleh dimanfaatkan untuk pengecualian luar biasa, termasuk kepada entiti tertentu seperti vendor teknologi, pihak ketiga luar negara, atau organisasi yang berkepentingan (Greenleaf, 2019; Morozov, 2011).

Lebih membimbangkan, akta ini tidak memperincikan kriteria atau skop pengecualian sama ada ia melibatkan syarikat swasta, agensi asing, atau kategori data tertentu. Ketiadaan sempadan ini membolehkan pengecualian dibuat atas justifikasi yang kabur atau bersifat politik, dan sekiranya tidak dipantau, ia berpotensi menjadi saluran sah kepada 'VIP Data Deals' yang membolehkan data tertentu dikecualikan daripada kawalan sistem sedia ada, di luar capaian audit, semakan keselamatan, atau justifikasi etika.

Dalam undang-undang negara lain yang menghargai prinsip pemisahan kuasa dan check-and-balance, kuasa pengecualian seperti ini biasanya memerlukan mekanisma semakan oleh badan legislatif atau kehakiman, atau sekurang-kurangnya laporan kepada jawatankuasa Parlimen (OECD, 2022; Tisne, 2020). Namun, Akta 864 tidak menyatakan keperluan pelaporan kepada PAC, JKICT, atau mana-mana badan pemantau bebas, menjadikan proses pengecualian ini berisiko dilakukan secara tertutup.

Dalam konteks daulat, peruntukan sebegini melemahkan keabsahan kuasa negara terhadap maklumat. Daulat dalam maklumat bukan terletak pada kebolehan memberi pengecualian, tetapi pada keupayaan mewujudkan sistem yang adil, telus, dan terhad kepada keperluan darurat sebenar. Tanpa batasan prinsipil, kuasa pengecualian akan berubah dari fleksibiliti kepada potensi penyalahgunaan.

Justeru, Seksyen 27 bukan hanya memerlukan reformulasi dari sudut teknikal, tetapi juga perlu diseimbangkan dengan mekanisma semak dan imbang institusional. Ini termasuk had ke atas siapa yang boleh dikecualikan, laporan awam berkala, dan proses justifikasi yang boleh diaudit. Tanpa ini, prinsip kedaulatan data yang ingin ditegakkan melalui Akta ini boleh diruntuhkan oleh satu pintu belakang yang sah di sisi undang-undang.

4.4 Ketiadaan klausa penyimpanan data berdaulat

Isu penyimpanan data bukan lagi persoalan teknikal semata-mata, tetapi menyentuh soal kedaulatan, keselamatan negara, dan kuasa jurisdiksi. Malangnya, dalam keseluruhan struktur Akta 864, tiada satu pun seksyen yang memperuntukkan bahawa data yang dikongsi antara agensi kerajaan perlu disimpan dalam pelayan fizikal milik negara atau dikawal secara sah oleh entiti tempatan.

Ketiadaan klausa penyimpanan data berdaulat (*sovereign data hosting*) ini menimbulkan kebimbangan yang serius. Tanpa keperluan penyimpanan dalam pelayan tempatan atau sekurang-kurangnya dalam *cloud* yang tertakluk kepada undang-undang Malaysia, data berisiko disimpan di luar negara, tertakluk kepada perundangan asing seperti *CLOUD Act* di Amerika Syarikat, atau mungkin dikendalikan oleh vendor teknologi yang tidak terikat dengan prinsip dan nilai domestik (Kuner, 2015b; Chander & Le, 2014).

Data yang disimpan di luar sempadan negara, terutamanya data awam berskala besar seperti kesihatan, pendidikan, dan infrastruktur boleh dijadikan bahan analisis luar yang tidak dapat dikesan, disekat, atau dikawal. Negara tidak lagi memiliki kawalan penuh ke atas siapa yang boleh mengakses, menganalisis, atau memindahkan data tersebut, dan jurisdiksi Malaysia menjadi tidak berfungsi dalam ruang digital antarabangsa.

Negara-negara yang serius mempertahankan kedaulatan maklumat mereka telah mula mewajibkan pelaksanaan *data localization* atau *sovereign cloud* seperti yang dilakukan di China, Rusia, dan Kesatuan Eropah. Malah Singapura telah menggerakkan dasar *data residency* untuk sistem kritikal kerajaan, memastikan bahawa semua data sensitif kekal berada dalam ekosistem yang boleh diaudit dan dilindungi

sepenuhnya (Greenleaf, 2019; Zeng et al., 2021).
Dalam konteks Malaysia, beberapa inisiatif awal seperti pembangunan Pusat Data Nasional dan penyediaan *Cloud Sovereign Framework* telah disebut dalam dokumen MyDigital. Namun, Akta 864 tidak mengambil kesempatan untuk mewajibkan penyimpanan data strategik dalam persekitaran berdaulat sebagai syarat perkongsian antara agensi. Hal ini menimbulkan persoalan sama ada akta ini benar-benar diselaraskan dengan agenda digital nasional, atau sekadar mempercepatkan aliran data tanpa membina benteng ketahanan maklumat.

Dari perspektif kedaulatan data, penyimpanan ialah akar kuasa. Jika data ialah "darah" digital negara, maka pelayan dan *cloud* ialah "jantung" yang menampungnya. Negara yang tidak tahu di mana datanya disimpan, tidak akan tahu siapa yang sedang mengawalnya. Maka, ketiadaan klausa penyimpanan data berdaulat bukan sekadar kekurangan teknikal, tetapi titik kelemahan strategik yang boleh melemahkan seluruh kedaulatan digital negara.

4.5 Tiada takrif data strategik negara

Salah satu kekosongan mendasar dalam Akta 864 ialah ketiadaan takrif rasmi atau klasifikasi terhadap apa yang dianggap sebagai "data strategik negara." Akta ini memperlakukan semua data yang dikongsi antara agensi kerajaan sebagai entiti yang setara dari sudut kawalan dan nilai strategik, tanpa membezakan antara maklumat biasa seperti data kehadiran sekolah dengan maklumat kritikal seperti lokasi pelaburan strategik, sumber pertahanan, atau peta risiko keselamatan siber negara.

Ketiadaan takrif ini bermakna tiada keperluan perundangan untuk memberi lapisan perlindungan tambahan terhadap data yang berisiko tinggi. Akibatnya, potensi untuk data sensitif dikongsi tanpa klasifikasi, kawalan akses bertingkat, atau justifikasi keselamatan yang teliti menjadi sangat tinggi. Ini bukan sekadar kelalaian, tetapi kegagalan untuk mengenalpasti apa yang mesti dipertahankan lebih keras daripada yang lain.

Negara-negara yang serius dalam mempertahankan kepentingan maklumat nasional telah pun menggerakkan dasar klasifikasi data strategik. Sebagai contoh, China melalui Undang-Undang Keselamatan Data 2021 memperkenalkan sistem pengelasan data (*data classification*) di mana maklumat dikategorikan kepada "*core data*," "*important data*," dan "ordinary data" yang mana masing-masing tertakluk kepada tahap kawalan yang berbeza (Zeng et al., 2021). Begitu juga Kesatuan Eropah melalui Akta Tadbir Urus Data (Data Governance Act) menekankan keperluan pelabelan maklumat berasaskan risiko dan sensitiviti.

Tanpa mekanisma pengenalpastian seperti ini, Malaysia akan terus beroperasi dalam kesamaran di mana maklumat strategik boleh dikongsi tanpa sedar, tanpa jejak klasifikasi, dan tanpa protokol mitigasi kebocoran. Ini amat membimbangkan apabila melibatkan data berkaitan:

- Infrastruktur kritikal negara (air, tenaga, komunikasi),
- Pergerakan aset pertahanan,
- Dana kekayaan negara (*sovereign wealth funds*),
- Biodiversiti dan sumber genetik,
- Kawasan pelaburan berisiko tinggi.

Lebih daripada itu, dalam kerangka maqasid syariah, salah satu prinsip utama ialah hifz al-mal (menjaga harta) dan hifz al-din wa al-ard (menjaga agama dan tanah air). Data yang menggambarkan sistem sokongan sosial, institusi agama, dan sumber tempatan ialah harta maklumat bangsa yang wajib dipelihara dengan lebih ketat berbanding maklumat rutin pentadbiran. Ketiadaan klasifikasi strategik ini bermaksud tiada beza antara emas dengan batu kerikil dalam sistem maklumat negara.

Oleh itu, kelemahan ini menandakan perlunya pindaan struktur kepada Akta 864, agar diwujudkan satu sistem pelabelan dan klasifikasi data nasional berasaskan sensitiviti, implikasi keselamatan, dan nilai strategik terhadap kepentingan negara. Tanpa ini, negara mempertaruhkan kedaulatan maklumat negara atas dasar ketidakpastian yang disengajakan.

4.6 Tiada mekanisme semak dan imbang awam

Dalam sistem demokrasi yang berfungsi, setiap bentuk kuasa terutama kuasa terhadap maklumat mesti disertakan dengan mekanisma semak dan imbang (*checks and balances*). Namun, salah satu kelemahan paling ketara dalam Akta 864 ialah ketiadaan peruntukan yang memperuntukkan pengawasan bebas atau pemantauan awam terhadap operasi, keputusan, dan impak daripada proses perkongsian data antara agensi.

Akta ini memberikan kuasa besar kepada Jawatankuasa Perkongsian Data Negara (Seksyen 5) untuk menetapkan keputusan dasar, menilai permintaan data, dan memutuskan kelulusan atau penolakan, tetapi tidak mewajibkan laporan tahunan, audit bebas, atau pemakluman kepada Parlimen. Tiada klausa yang menetapkan bahawa aktiviti jawatankuasa ini perlu dilaporkan kepada PAC, Jawatankuasa Khas Teknologi, atau mana-mana entiti semak yang neutral dari pengaruh eksekutif.

Lebih mengganggu, tiada keperluan untuk menerbitkan statistik berkenaan:

- Jumlah data yang telah dikongsi,
- Kategori data yang paling banyak diproses,
- Agensi yang menerima dan meminta data terbanyak,
- Tujuan utama permintaan data.

Ketiadaan keperluan pelaporan ini mengakibatkan “ruang gelap” dalam pengurusan maklumat awam, di mana keputusan boleh dibuat tanpa sebarang proses pemberitahuan kepada rakyat. Dalam konteks digital, ini membuka jalan kepada apa yang digambarkan oleh Shoshana Zuboff sebagai “*instrumentarian power*” kuasa yang mengawal tanpa ketara, memproses tanpa didedah, dan mempengaruhi tanpa dialog (Zuboff, 2019).
Dari perspektif Islam dan prinsip syura, kuasa yang tidak dipantau bukanlah kuasa yang sah. Amanah mesti disertai dengan hisbah, iaitu sistem teguran dan pemantauan yang memastikan keadilan terpelihara. Tanpa elemen ini, kedaulatan digital berubah menjadi bentuk autoritarianisme algoritmik, di mana rakyat tidak tahu siapa yang mengawal data mereka, untuk apa, dan sejauh mana data itu telah mengubah kehidupan mereka tanpa pengetahuan.

Beberapa negara telah mengambil langkah proaktif untuk menangani isu ini. Di UK dan Australia, sebarang pemprosesan data awam oleh agensi kerajaan tertakluk kepada *Data Impact Assessments (DIA)* yang perlu diterbitkan secara terbuka sebelum pelaksanaan. Di EU, *Data Protection Authorities (DPA*) memiliki kuasa bebas untuk menyemak dan mengaudit mana-mana operasi perkongsian maklumat, termasuk yang melibatkan agensi kerajaan tertinggi (European Commission, 2020b; OECD, 2022).

Ketiadaan mekanisma ini dalam Akta 864 menimbulkan persoalan kritikal: Siapa yang akan memantau pemantau? Dan jika tiada entiti luar yang boleh mengaudit pengurus maklumat negara, di manakah ruang rakyat untuk bersuara dan mencabar penyalahgunaan kuasa?

Justeru, kelemahan ini bukan sahaja bersifat teknikal, tetapi juga mengganggu asas legitimasi moral dan demokratik terhadap daulat digital negara. Kedaulatan yang sebenar bukan sahaja berkaitan siapa yang mengawal, tetapi juga siapa yang boleh menyoal kawalan itu.

5.0 Implikasi terhadap Kuasa Nasional dalam Era Maklumat

Kedaulatan data bukan sekadar isu kecekapan pentadbiran atau pemodenan teknologi. Ia adalah medan baru perebutan kuasa, di mana kekuatan sesebuah negara semakin ditentukan bukan hanya oleh senjata, sumber asli atau sempadan geografi, tetapi oleh keupayaannya mengawal maklumat, mentakrif makna, dan mempertahankan naratifnya sendiri. Data telah menjadi struktur asas kepada segala bentuk perancangan, pemantauan, pembuatan keputusan dan, yang paling halus tetapi berbahaya, pengaruh ke atas kesedaran kolektif sesebuah masyarakat.

Oleh itu, kelemahan struktur dalam Akta 864 bukan boleh dinilai dari sudut undang-undang pentadbiran semata-mata. Ia perlu diteliti sebagai tanda awal kepada potensi pelonggaran kuasa nasional, di mana sistem yang dibina tanpa sempadan nilai dan pengawasan berisiko melucutkan negara daripada instrumen-

instrumen kuasa yang paling senyap tetapi paling menentukan, iaitu maklumat. Lebih penting, apabila data strategik tidak lagi dimiliki, disimpan atau ditafsir oleh negara sendiri, maka kuasa negara terhadap takrifan kebenaran, hala tuju pembangunan, dan identiti kolektif akan turut terhakis secara perlahan tetapi menyeluruh.

Dalam konteks ini, mesti diakui bahawa kehilangan data ialah kehilangan kuasa. Dan kehilangan kuasa terhadap data adalah lebih berbahaya berbanding kehilangan senjata, kerana ia tidak menumpahkan darah tetapi menghapuskan arah.

Seksyen ini akan menghuraikan lima bentuk implikasi besar terhadap kuasa nasional yang muncul apabila prinsip kedaulatan data tidak ditangani secara menyeluruh dan berprinsip. Ia bukan sekadar analisis kelemahan dasar, tetapi satu amaran bahawa tanpa kawalan terhadap ruang digital, tidak ada negara yang benar-benar berdaulat.

5.1 Kehilangan jurisdiksi digital sebagai kehilangan wilayah kuasa

Dalam tradisi geopolitik klasik, kehilangan tanah bermakna kehilangan kedaulatan. Namun dalam era digital, wilayah tidak lagi diukur melalui sempadan fizikal, tetapi melalui batasan kawalan ke atas data dan infrastruktur maklumat. Jurisdiksi digital iaitu keupayaan undang-undang sesebuah negara untuk mengawal, mengakses dan melindungi data rakyatnya telah menjadi bentuk baharu wilayah kedaulatan. Malangnya, ia juga merupakan bentuk wilayah yang paling mudah tergelincir dari genggaman, kerana ia tidak kelihatan, tidak berbunyi, dan tidak terbendung jika tiada kehendak politik untuk menahannya.

Kegagalan negara untuk mewujudkan "*data sovereignty regime*" yang kukuh bermakna sebahagian besar data rakyat termasuk data peribadi, maklumat kesihatan, lokasi, perbankan, tingkah laku sosial dan pelbagai aset maklumat awam, boleh bergerak merentas sempadan tanpa kawalan, disimpan di pelayan asing, dan terdedah kepada jurisdiksi luar seperti US CLOUD Act (Kuner, 2015b; Chander & Le, 2014). Situasi ini bukan hanya menghakis kawalan negara terhadap privasi dan keselamatan, tetapi melumpuhkan kuasa penguatkuasaan undang-undang domestik dalam ruang digital yang dikawal oleh entiti luar.

Kesannya amat nyata, apabila data disimpan di pelayan luar negara, sebarang siasatan, semakan atau tindakan ke atas pelanggaran hanya boleh dilakukan jika negara berkenaan bersetuju untuk bekerjasama dan ini tertakluk kepada kepentingan politik, undang-undang, serta diplomasi dua hala. Hal ini digambarkan sebagai "*jurisdictional dislocation*", di mana negara menjadi buta terhadap data sendiri kerana kuasa akses tidak lagi berada di tangan mereka (Bradshaw, Millard & Walden, 2011; Tikk & Kerttunen, 2020).

Lebih serius, sesetengah negara seperti Amerika Syarikat secara terang-terangan mengiktiraf hak mereka untuk mengakses data yang disimpan oleh syarikat teknologi mereka walaupun pelayan tersebut berada di negara lain. Ini diperuntukkan secara sah dalam *CLOUD Act 2018*, yang memberi kuasa kepada kerajaan AS untuk menuntut akses kepada data dari *Microsoft, Google, Amazon* dan *Apple* walaupun data itu disimpan di luar Amerika Syarikat (Swire & Hemmings, 2019). Maka jika kerajaan Malaysia menyimpan data awam dalam sistem awan global yang dikendalikan oleh vendor-vendor ini, jurisdiksi ke atas data tersebut secara praktiknya telah beralih ke tangan negara lain.

Dalam konteks ini, kehilangan jurisdiksi digital bukan sekadar kelemahan teknikal, tetapi kehilangan kawalan terhadap kuasa eksekutif negara itu sendiri. Ia menggugat keupayaan negara untuk menyiasat jenayah, melindungi rakyat, mengawasi sistem pentadbiran dan memastikan keadilan maklumat kerana mekanisma undang-undang tempatan tidak lagi boleh dikuatkuasakan ke atas data yang terletak di luar kawalan fizikal dan undang-undang negara (Kuner, 2015b; Klimburg, 2017).

Fenomena ini juga memberi kesan besar kepada keselamatan nasional. Dalam laporan *Data Sovereignty and Cybersecurity* oleh OECD, dinyatakan bahawa negara yang tidak memiliki kawalan ke atas pelayan tempatan akan lebih rentan terhadap sabotaj siber, pengintipan digital, dan penyalahgunaan sistem oleh aktor luar kerana *"they are unable to exercise full security protocols without infrastructure control"* (OECD, 2022). Oleh itu, ketidakupayaan untuk menuntut jurisdiksi penuh ke atas maklumat digital sama seperti membenarkan aktor luar menguasai sebahagian daripada sistem saraf negara.

Apa yang lebih membimbangkan, negara-negara membangun seperti Malaysia sering kali terjerat dalam pergantungan teknologi yang menghalang usaha membina alternatif. Ini menyebabkan mereka terpaksa

menukar kedaulatan dengan kemudahan, menyerahkan kawalan demi kelajuan pelaksanaan, dan akhirnya menjadi pengguna dalam sistem yang mereka sendiri tidak boleh bentuk atau semak.

Maka, jurisdiksi digital ialah wajah baharu kepada sempadan negara. Dan negara yang tidak memiliki atau mempertahankan sempadan ini akan kehilangan bukan sahaja data, tetapi kuasa untuk mentadbir, melindungi dan memimpin. Dalam bahasa yang lebih dalam, ia adalah kehilangan kuasa untuk mengatakan "tidak" dalam ruang maklumat. Dan apabila sebuah negara hilang kuasa untuk mengatakan tidak, maka yang tinggal hanyalah ilusi kedaulatan, tanpa gigi, tanpa sempadan, tanpa wibawa.

5.2 Ketidakmampuan negara mengawal arah, naratif dan realiti sosial sendiri

Kawalan terhadap data bermaksud kawalan terhadap makna. Dalam ekosistem digital yang membentuk hampir semua aspek kehidupan, daripada perbualan harian, pandangan politik, sehingga ke cara memahami sejarah dan masa depan, data ialah bahan mentah yang membina realiti. Tanpa kawalan terhadap data, negara akan kehilangan keupayaan untuk menentukan arah pembangunan, membentuk wacana nasional, dan memelihara integriti sosialnya.

Hari ini, algoritma yang digerakkan oleh data menentukan apa yang muncul di skrin rakyat, berita mana yang dianggap penting, dan naratif mana yang mendapat perhatian. Namun sistem ini tidak lagi dikawal oleh negara, tetapi oleh syarikat luar yang mempunyai agenda pasaran dan politik yang berbeza. Maka yang muncul di skrin bukan semestinya mencerminkan keperluan atau nilai tempatan, tetapi apa yang menguntungkan secara komersial atau dikehendaki oleh kuasa dominan pasaran data global.

Tanpa kawalan terhadap sumber maklumat dan proses penapisan, negara akan menjadi penumpang dalam kenderaan digital yang dipandu oleh pihak lain. Ia hanya mampu memberi reaksi, bukan menyusun strategi. Ini bukan sekadar kehilangan suara, tetapi kehilangan keupayaan untuk mencipta suara. Ia menjadikan rakyat lebih terdedah kepada pembentukan makna luar yang tidak selari dengan konteks budaya, sejarah dan nilai tempatan (Couldry & Mejias, 2019).

Fenomena ini pernah digambarkan oleh Shoshana Zuboff sebagai instrumentarian power, suatu bentuk kuasa baharu yang tidak memerlukan paksaan atau perundangan, kerana ia mengubah manusia melalui penstrukturan realiti berdasarkan pengurusan data. Dalam konteks negara, apabila naratif dibentuk oleh data yang tidak dimiliki, maka dasar, persepsi awam dan tindakan kerajaan akan sentiasa dikejar oleh bayangan yang dihasilkan luar kawalan (Zuboff, 2019).

Dalam dunia pasca-kebenaran, negara yang tidak memiliki sistem maklumatnya sendiri akan bergantung kepada tafsiran luar untuk memahami sendiri realiti dalam negaranya. Dalam erti kata lain, negara tidak lagi tahu apa yang sedang berlaku kepada rakyatnya melainkan melalui data yang dimiliki oleh pihak ketiga. Ia bukan hanya kehilangan data, tetapi kehilangan epistemologi cara mengetahui.

Tambahan pula, kehilangan kawalan naratif juga bermaksud kehilangan kawalan terhadap imaginasi masa depan. Siapa yang menguasai data, akan menguasai impian. Impian untuk menjadi negara unggul tidak akan berlaku jika pelan strategik dibina atas maklumat yang diproses oleh sistem luar, melalui algoritma yang tidak boleh diaudit secara dalaman (Tisne, 2020; Milan & Treré, 2019).

Lebih daripada itu, masyarakat yang tidak mengawal naratifnya sendiri akan terdedah kepada asimetri maklumat, di mana sesetengah kelompok luar lebih memahami struktur, tingkah laku dan kecenderungan sosial negara berbanding pemerintahannya sendiri. Dalam situasi ini, kerajaan berisiko membina dasar berasaskan ilusi, bukan realiti sebenar, kerana realiti tersebut telah “dipakejkan semula” oleh pihak yang mengawal datanya (Floridi, 2020).

Maka, kedaulatan data bukan sekadar soal simpanan maklumat, tetapi tentang siapa yang menulis cerita tentang negara. Negara yang tidak mengawal datanya, tidak akan mampu mengawal ceritanya. Dan apabila cerita itu tidak lagi milik sendiri, maka seluruh sistem nilai, pendidikan, ekonomi dan sosial akan berputar atas paksi yang dipilih oleh orang lain.

5.3 Ketirisan maklumat strategik dan krisis kepemilikan makna

Dalam sesebuah negara berdaulat, data tidak wajar dilihat secara homogen. Terdapat maklumat yang

bersifat rutin, dan ada pula yang bersifat strategik dan mengandungi nilai, rahsia, dan kuasa takrifan terhadap identiti, sumber, serta hala tuju kolektif. Ketirisan maklumat strategik tidak hanya melibatkan pelanggaran keselamatan siber, tetapi mencetuskan kehilangan hak mentafsir dan membina makna secara berdaulat.

Masalah utama berpunca daripada ketiadaan kerangka nasional yang jelas untuk mengklasifikasikan data strategik. Akta 864 tidak menetapkan definisi yang tuntas berkenaan kategori maklumat yang dianggap kritikal kepada keselamatan, ekonomi, atau keutuhan sosial negara. Akibatnya, kesemua jenis maklumat berisiko dikendalikan di bawah rejim kawalan yang sama, tanpa mengambil kira nilai strategik dan sensitiviti sesetengah data. Sehingga kini, Malaysia masih belum membangunkan kerangka pengkelasan data yang setara dengan model negara lain, apatah lagi yang berakar pada realiti dan keperluan tempatan.

Ketiadaan klasifikasi yang tuntas ini membuka ruang kepada pendedahan dan pemindahan maklumat yang memiliki nilai strategik, tanpa garis panduan atau had kawalan yang berasaskan prinsip. Apabila maklumat tersebut dikendalikan atau diproses oleh entiti luar, terutamanya syarikat teknologi global atau penyedia analitik rentas sempadan, risiko kehilangan kuasa pentafsiran meningkat secara signifikan. Dalam kerangka data colonialism, proses ini menyebabkan masyarakat kehilangan kuasa mentakrifkan dirinya sendiri apabila data diproses di luar kawalan nilai dan konteks asal (Couldry & Mejias, 2019).

Fenomena ini menimbulkan apa yang boleh disebut sebagai krisis kepemilikan makna. Data yang berasal dari komuniti tempatan, apabila dikendalikan oleh sistem asing, berisiko dimaknai semula berdasarkan logik pasaran atau keutamaan luar. Naratif pembangunan, identiti budaya, dan struktur sosial boleh disusun berdasarkan data yang telah dimanipulasi oleh algoritma yang tidak mengenal sensitiviti sejarah atau kerangka nilai asal.

Dari sudut falsafah ilmu Islam, makna dianggap sebagai keluaran dari interaksi antara konteks, adab, dan hikmah (al-Attas, 1978; Auda, 2008). Apabila maklumat dikendalikan di luar rantaian nilai ini, kebarangkalian untuk tafsiran menyimpang meningkat. Krisis makna bukan hanya berimplikasi kepada pemahaman, tetapi kepada dasar, kerana dasar dibina atas andaian, dan andaian terbentuk dari maklumat yang diproses.

Zuboff (2019) pula menegaskan bahawa instrumentarian power muncul apabila data digunakan bukan untuk pemahaman, tetapi untuk pembentukan tingkah laku secara senyap. Kehilangan kawalan terhadap data strategik menyebabkan pelbagai bentuk Keputusan termasuk dalam pendidikan, pembangunan ekonomi, atau struktur nilai disandarkan pada maklumat yang tidak mencerminkan realiti asal.

Oleh yang demikian, keupayaan untuk mempertahankan makna bergantung kepada keupayaan untuk mengenalpasti dan melindungi maklumat strategik. Langkah awal ke arah kedaulatan maklumat melibatkan proses sistematik pengenalpastian, klasifikasi, dan kawalan terhadap data bernilai tinggi berdasarkan konteks, bukan semata-mata berdasarkan standard universal. Tanpa kerangka ini, maklumat yang paling penting berisiko besar terdedah, dimiliki, dan dimaknai oleh pihak luar tanpa sebarang rujukan kepada struktur makna asal.

5.4 Ketergantungan sistemik terhadap ekosistem digital luar

Ketergantungan terhadap ekosistem digital luar merupakan salah satu bentuk dominasi senyap yang paling ketara dalam landskap maklumat masa kini. Kebergantungan terhadap platform, penyimpanan data, sistem awan, serta perisian yang dibangunkan dan dikendalikan oleh entiti luar telah melahirkan satu bentuk pergantungan struktural yang sukar dibebaskan, baik dari segi teknikal, perundangan, mahupun ideologi (Chander & Le, 2014; Souter, 2020).

Malaysia, seperti banyak negara lain di rantau Global South, masih bergantung kepada penyedia perkhidmatan teknologi maklumat global seperti *Amazon Web Services, Microsoft Azure, Google Cloud,* dan pelbagai vendor sistem pengurusan data antarabangsa yang tidak berpangkalan secara sah dalam sistem perundangan tempatan (UNCTAD, 2021). Situasi ini menimbulkan risiko besar apabila data awam, termasuk yang bernilai strategik, disimpan dalam pelayan yang tertakluk kepada undang-undang negara asal penyedia perkhidmatan, bukan di bawah bidang kuasa Malaysia.

Masalah ini bukan sekadar teknikal, tetapi bersifat struktural dan sistemik. Ekosistem digital global telah dibina secara asimetrik, di mana negara maju membentuk standard, piawaian, dan struktur pasaran,

sementara negara membangun menjadi pengguna dan penerima yang pasif (Gurumurthy & Chami, 2020a). Dalam jangka panjang, model ini bukan sahaja melemahkan pembangunan teknologi tempatan, tetapi juga membina ketakupayaan strategik untuk bertindak secara bebas dalam pengurusan maklumat awam.

Lebih membimbangkan, ketergantungan ini melahirkan apa yang disebut oleh Milan & Treré (2019) sebagai data universalism, iaitu kecenderungan untuk menganggap satu sistem sesuai untuk semua konteks, tanpa mengambil kira nilai, sejarah, dan realiti setempat. Apabila penyelesaian teknologi dibentuk berdasarkan logik luaran, risiko pengabaian terhadap sensitiviti budaya, bahasa, dan sistem nilai tempatan menjadi tinggi. Ini menjadikan proses digitalisasi negara lebih bersifat importasi sistem, bukan transformasi berpandukan kendiri.

Tanpa infrastruktur data berdaulat, negara kehilangan keupayaan untuk melindungi integriti maklumat, mengawal aliran data, dan membina inovasi berdasarkan realiti domestik. Usaha Malaysia melalui Rangka Tindakan MyDigital dan perancangan Pusat Data Nasional masih dilihat belum mencukupi tanpa pelaksanaan undang-undang yang mewajibkan penyimpanan data strategik dalam lingkungan jurisdiksi tempatan (MyDigital, 2021). Tambahan pula, ketiadaan klausa data localization dalam Akta 864 menjadikan ia tidak seiring dengan keperluan membina ekosistem maklumat yang tahan lasak secara geopolitik.

Ketergantungan digital dalam konteks ini tidak boleh dilihat hanya sebagai isu kecekapan atau kos operasi. Ia ialah bentuk infra-kolonialisme moden di mana asas kuasa negara ditentukan oleh kebergantungan terhadap infrastruktur yang tidak dimiliki. Oleh itu, kebebasan maklumat bukan akan dicapai melalui akses kepada teknologi semata-mata, tetapi melalui pembinaan sistem maklumat yang bersifat kendiri, boleh audit, dan tertakluk sepenuhnya kepada perundangan dan nilai negara.

5.5 Melemahkan keupayaan kolektif membina kuasa peradaban sendiri

Dalam ekosistem global yang dipacu data, kemampuan sesebuah negara untuk membina struktur pengetahuan, arah pembangunan dan naratif sosialnya sendiri tidak lagi bergantung sepenuhnya kepada sumber material semata-mata, tetapi bergantung pada keupayaannya mengurus dan mentakrif maklumat. Kehilangan keupayaan untuk berbuat demikian, sama ada melalui kebocoran, kebergantungan, atau kehilangan kedaulatan maklumat merupakan bentuk kehilangan kuasa struktur yang paling subtil, namun paling mendasar.

Bentuk kebergantungan terhadap infrastruktur data luar bukan hanya mengundang ketirisan teknikal, tetapi juga mencipta apa yang disebut sebagai "*epistemic asymmetry*", iaitu ketidakseimbangan dalam siapa yang berhak memahami, mentafsir dan membina makna sosial melalui data yang dikumpul (Floridi, 2020; Milan & Treré, 2019b). Apabila data awam yang merangkumi sejarah, budaya, interaksi sosial, dan struktur nilai sesebuah masyarakat dikendalikan oleh entiti luar, proses mentakrif realiti akan dikuasai oleh piawaian dan logik yang tidak berakar pada sistem nilai tempatan.

Dalam konteks pembangunan nasional, kebergantungan ini menghasilkan satu bentuk "*structural dependency*", di mana negara menjadi pengguna kepada teknologi maklumat luar tanpa memiliki agensi dalam membentuk arah reka bentuk, standard dan penilaian terhadap apa yang dikira sebagai "kemajuan" (Gurumurthy & Chami, 2020b). Apabila data tempatan digunakan untuk melatih sistem kecerdasan buatan luar, membina analitik luar negara, atau dimanfaatkan oleh pihak luar untuk dasar luar mereka sendiri, maka kehilangan agensi epistemik ini tidak lagi bersifat teori, tetapi menjadi bentuk kolonialisme maklumat yang realiti (Sadowski, 2019; Zuboff, 2019).

Fenomena ini menghalang pembentukan naratif tandingan atau sistem ilmu yang berpaksikan kepada pengalaman, keutamaan dan nilai setempat. Dalam kerangka teori *coloniality of knowledge*, dominasi struktur maklumat membawa kepada penggantian sistem ilmu lokal dengan sistem tafsiran luar yang berkuasa, satu bentuk penapisan makna yang menjejaskan potensi pembinaan masa depan yang berdikari secara epistemik (Quijano, 2000; Fricker, 2007). Dalam erti kata lain, pembangunan digital yang tidak berpaksikan kedaulatan data berisiko menghasilkan teknologi tanpa kendiri, dan dasar tanpa akar.

Tambahan pula, apabila negara kekal dalam posisi pasif sebagai penyumbang data dan pengguna sistem, keupayaan kolektif untuk membina model alternatif terhadap pembangunan dan arah strategik nasional menjadi semakin lemah. Bukan hanya keputusan dasar akan bergantung kepada model analitik luar, malah sistem pendidikan, kajian sosial, dan pembangunan ekonomi akan dibentuk berdasarkan tafsiran yang tidak

mencerminkan realiti domestik sebuah situasi yang disebut sebagai "*data dependency trap*" (Taylor, 2021).

Tanpa ekosistem data berdaulat, apa yang terbina hanyalah penyampaian maklumat, bukan pembinaan makna. Apa yang wujud hanyalah pengguna teknologi, bukan pemilik naratif. Maka, sebarang perundangan yang menyentuh data, termasuk Akta 864, tidak wajar hanya dinilai dari sudut kecekapan pentadbiran, tetapi mesti dianalisis dari segi bagaimana ia membantu atau menghalang keupayaan strategik sesebuah masyarakat untuk mentakrif dirinya sendiri dalam jangka panjang.

6.0 Cadangan penambahbaikan terhadap Akta Perkongsian Data 2025

Kedaulatan data pada asasnya bukan hanya soal keupayaan teknikal untuk menyimpan atau mengurus maklumat, tetapi suatu bentuk keupayaan normatif dan institusional yang membolehkan negara menentukan sempadan, standard, dan tafsiran terhadap maklumat yang dimilikinya. Dalam konteks global yang semakin didominasi oleh infrastruktur digital luar dan piawaian korporat rentas negara, struktur undang-undang domestik menjadi alat kritikal untuk mempertahankan agensi maklumat sesebuah negara. Seperti yang dihujahkan oleh Kuner (2015a), tanpa jurisdiksi digital yang jelas, negara akan kehilangan bukan sahaja kawalan terhadap maklumat, tetapi juga keupayaan untuk menguatkuasakan undang-undangnya sendiri.

Sebagaimana dihuraikan dalam seksyen-seksyen terdahulu, Akta 864 merupakan langkah awal ke arah rasionalisasi perkongsian data dalam sektor awam. Namun, seperti yang dinyatakan oleh Couldry dan Mejias (2019), tanpa struktur kawalan dan sempadan nilai yang kukuh, sistem perkongsian data boleh bertukar menjadi instrumen eksploitasi maklumat, bukan penguatan negara. Dalam kerangka tersebut, kelemahan-kelemahan yang dikenal pasti, seperti ketiadaan klasifikasi maklumat strategik, ketidakhadiran klausa penyimpanan data berdaulat, dan kuasa pengecualian menteri tanpa mekanisma semak dan imbang, tidak boleh dilihat sebagai isu pentadbiran semata-mata, tetapi sebagai petunjuk awal kepada potensi kehilangan kedaulatan maklumat secara struktural.

Tisne (2020) menyatakan bahawa ancaman terhadap hak data pada zaman ini bukan lagi bersifat individu, tetapi kolektif, kerana seluruh masyarakat boleh dimanipulasi melalui ekosistem data yang tidak dikawal oleh prinsip kebertanggungjawaban dan kejelasan kuasa. Penambahbaikan terhadap Akta 864 perlu dilihat sebagai peluang untuk membentuk bukan sahaja sistem yang efisien, tetapi juga sistem yang adil dan berdaulat secara prinsip. Ini seiring dengan gagasan bahawa undang-undang digital bukan semata-mata peraturan teknikal, tetapi instrumen penstrukturan kuasa, baik dalam dimensi pentadbiran mahupun epistemik (Zuboff, 2019; Taylor, 2021).

Sebahagian daripada cadangan ini mengambil inspirasi daripada amalan global seperti *Data Security Law China,* yang mengklasifikasikan data berdasarkan tahap sensitiviti dan impaknya terhadap keselamatan nasional (Zeng, Stevens & Chen, 2021), serta *Data Governance Act European Union*, yang memperkenalkan mekanisma tadbir urus bagi *high-value datasets* yang tidak boleh dikendalikan secara sewenang-wenangnya (European Commission, 2020a). Namun, penyesuaian terhadap konteks Malaysia memerlukan pendekatan yang lebih reflektif, dengan mempertimbangkan struktur nilai, sejarah perundangan, dan realiti teknokratik tempatan.

Akhirnya, sebagaimana yang dihujahkan oleh Milan dan Treré (2019), sistem data yang tidak berpaksikan kendiri akan menjadikan negara bergantung kepada logik universal yang tidak neutral, dan sering kali meminggirkan realiti masyarakat selatan global. Justeru, seksyen ini mengemukakan enam cadangan utama yang bukan sahaja menyasar kepada pengukuhan literal terhadap Akta Perkongsian Data 2025, tetapi juga ke arah pembangunan sistem maklumat nasional yang berpaksikan nilai, prinsip, dan struktur kuasa yang lebih adil, lestari, dan tahan terhadap manipulasi luaran.

6.1 Pewartaan kategori data strategik negara

Dunia hari ini melihat maklumat sebagai teras kuasa strategik, keupayaan sesebuah negara untuk mengawal dan mengklasifikasikan data mengikut nilai strategiknya merupakan prasyarat kepada kedaulatan digital (Floridi, 2020; Zuboff, 2019). Namun begitu, Akta 864 tidak menyediakan sebarang mekanisma pewartaan atau pengkategorian data berdasarkan tahap sensitiviti, impak keselamatan, atau nilai strategik terhadap negara. Hal ini mencetuskan risiko serius terhadap keselamatan maklumat, hak kendiri negara, dan integriti dasar awam, terutama apabila maklumat dikongsi secara seragam tanpa

klasifikasi berasaskan risiko (Kuner, 2015b; Taylor, 2021).

Pengelasan data bukanlah isu teknikal semata, tetapi berkait dengan prinsip epistemik dan struktur kuasa negara. Tanpa klasifikasi rasmi, negara kehilangan keupayaan untuk membina sistem maklumat yang bersifat hierarki dan reflektif kepada keperluan keselamatan dan budaya maklumatnya sendiri (Couldry & Mejias, 2019; Milan & Treré, 2019). Tambahan pula, pewartaan data strategik membolehkan kerajaan melabur dengan lebih efisien ke atas infrastruktur perlindungan maklumat berisiko tinggi, sekaligus menyusun keutamaan nasional secara lebih bermakna (Bharadwaj et al., 2022; Hummel, Braun & Dabrock, 2021b).

Lebih kritikal, pewartaan data strategik juga menjadi asas kepada pelaksanaan "*data localization*", di mana sesetengah data hanya boleh disimpan dan diproses dalam sempadan negara. Ini penting untuk melindungi data seperti pelaburan GLC, peta aset pertahanan, salasilah warga, dan rekod bio-warisan negara yang jika jatuh ke tangan asing, boleh menjejaskan keselamatan, reputasi, atau ekonomi nasional (De Filippi & Greenstein, 2020; United Nations, 2022). Malah, laporan OECD (2021) menekankan bahawa ketiadaan klasifikasi maklumat strategik menyebabkan negara terdedah kepada manipulasi algoritma luar terhadap data domestik.

Oleh itu, dicadangkan agar Akta 864 dipinda untuk memperkenalkan satu kerangka pewartaan rasmi terhadap data strategik negara. Pewartaan ini harus mengandungi sekurang-kurangnya tiga kategori:

1. Data Kritikal Negara (DKN) – seperti lokasi pertahanan, identiti keselamatan, data operasi strategik.
2. Data Sensitif Awam (DSA) – seperti maklumat kesihatan, sosial, pendidikan, zakat dan wakaf.
3. Data Umum Terkawal (DUT) – termasuk data statistik, perkhidmatan kerajaan, logistik, dsb.

Penggubalan kategori ini mesti dipandu oleh satu panel antara agensi melibatkan Jabatan Digital Negara, Agensi Keselamatan Siber, MKN, SKMM dan juga sektor sivil dan akademik. Ia mesti diwartakan secara sah, dengan prosedur audit, kawalan akses, dan penalti jelas untuk setiap kategori (UNCTAD, 2022).

Dalam jangka panjang, pewartaan data strategik bukan sahaja melindungi nilai maklumat nasional, tetapi juga membina ekosistem kepercayaan antara kerajaan dan rakyat. Ia menzahirkan prinsip bahawa data bukan sekadar alat pentadbiran, tetapi amanah negara yang perlu diurus secara bermaruah dan berdaulat (Taylor, 2021; Zuboff, 2019).

6.2 Klausa penyimpanan data berdaulat dan keperluan infrastruktur tempatan

Penyimpanan data dalam sempadan negara merupakan elemen utama dalam menegakkan kedaulatan data. Tanpa kawalan terhadap lokasi, akses, dan infrastruktur pemprosesan data, sesebuah negara kehilangan keupayaan untuk memastikan bahawa maklumat sensitif tidak tertakluk kepada jurisdiksi asing atau manipulasi teknikal luar (Kuner, 2015b; Gurumurthy & Chami, 2020a). Dalam konteks Akta 864, ketiadaan sebarang klausa yang mewajibkan penyimpanan data strategik dalam infrastruktur yang dikawal secara tempatan menimbulkan kebimbangan terhadap kebocoran maklumat kritikal dan kehilangan autonomi dalam ruang digital negara.

China, sebagai antara pelopor dasar cyber-sovereignty, telah mewajibkan penyimpanan domestik bagi data penting melalui *Cybersecurity Law (2017)* dan memperkuatkannya melalui *Data Security Law (2021)*, yang mengkehendaki audit keselamatan dan kelulusan kerajaan sebelum sebarang pemindahan rentas sempadan bagi data penting dilakukan (Zeng, Stevens & Chen, 2021). Kesatuan Eropah pula melalui *European Data Strategy* menekankan keperluan membina *European Gaia-X Cloud Infrastructure*, bagi memastikan kawalan terhadap data awam dan industri kekal dalam lingkungan EU (European Commission, 2020a).

Lebih mendalam lagi, penyimpanan data berdaulat bukan sekadar soal lokasi fizikal pelayan, tetapi berkaitan dengan siapa yang memiliki, mengawal, dan boleh mengakses sistem itu. Seperti yang dihuraikan oleh Floridi (2020), kedaulatan digital memerlukan "*control over the informational substrate*" yakni asas teknikal kepada semua bentuk kuasa maklumat. Oleh itu, pemilikan infrastruktur digital oleh syarikat luar, walaupun fizikalnya berada di dalam negara, masih tidak menjamin keselamatan maklumat negara jika kunci penyulitan, protokol kawalan akses, dan audit log dimiliki entiti asing (Sadowski, 2019; Hummel et al., 2021a).

Tanpa peruntukan undang-undang yang mewajibkan data strategik negara disimpan di pelayan milik tempatan, usaha untuk menubuhkan pusat data nasional tidak akan membawa impak strategik yang sebenar. Malah, dalam ketiadaan klausa penyimpanan berdaulat, data kerajaan yang dikongsi antara agensi berpotensi disalurkan ke infrastruktur yang tidak diketahui pemilik atau rantai kawalannya.

Sehubungan itu, Akta 864 perlu dipinda untuk memasukkan klausa wajib penyimpanan data dalam pelayan fizikal milik kerajaan atau entiti yang ditetapkan secara rasmi di bawah undang-undang Malaysia. Klausa ini boleh disusun mengikut tiga tahap:

1. Tahap 1 – Data Kritikal: Mesti disimpan dalam pelayan kerajaan dengan kawalan keselamatan penuh.
2. Tahap 2 – Data Sensitif: Boleh disimpan di pelayan tempatan milik vendor yang berpangkalan di Malaysia dengan audit keselamatan berkala.
3. Tahap 3 – Data Biasa: Terbuka untuk penyimpanan awan, tetapi mesti memenuhi kriteria ketelusan, enkripsi dan pelaporan akses.

Klausa ini juga perlu disokong oleh pembangunan *Sovereign Cloud Infrastructure*, yang tidak hanya bersifat fizikal tetapi bersandarkan kepada prinsip keboleh-auditan, keterkawalan tempatan, dan kesetiaan terhadap undang-undang kebangsaan (Tisne, 2020; DeNardis, 2014). Tanpa struktur ini, agenda digitalisasi negara hanya akan mempercepatkan ketergantungan terhadap sistem luar tanpa jaminan kedaulatan maklumat sebenar.

6.3 Pengukuhan semak dan imbang melalui pelaporan parlimen dan audit bebas

Kedaulatan maklumat dalam konteks negara demokrasi moden tidak hanya diukur melalui keupayaan mengawal infrastruktur atau memegang pemilikan data, tetapi juga melalui kewujudan sistem semak dan imbang yang berfungsi dan telus. Dalam konteks Akta 864, Seksyen 27 memperuntukkan kuasa kepada menteri untuk mengecualikan mana-mana pihak daripada peruntukan akta ini, tanpa mewajibkan sebarang pelaporan berkala atau mekanisma pengesahan rentas institusi. Peruntukan ini secara tidak langsung menimbulkan risiko terhadap prinsip kebertanggungjawaban (*accountability*) dan boleh membawa kepada amalan pengecualian secara tertutup, yang melemahkan kredibiliti dan integriti tadbir urus data kerajaan (Floridi, 2020; Taylor, 2021).

Amalan semak dan imbang terhadap kuasa eksekutif dalam pentadbiran maklumat awam telah menjadi prinsip asas dalam sistem demokrasi maklumat (Bannister & Connolly, 2012). Dalam kes-kes seperti United Kingdom, kuasa pengurusan data awam berada di bawah pantauan Information Commissioner's Office (ICO) yang memiliki kuasa statutori untuk meneliti proses perkongsian dan penggunaan data awam (ICO, 2023). Begitu juga dengan Data Governance Act Kesatuan Eropah yang menetapkan agar pelaporan tahunan dan audit pihak ketiga menjadi prasyarat kepada perkongsian data strategik antara negara anggota (European Commission, 2020a).

Ketiadaan mekanisma audit bebas dalam Akta 864 juga bercanggah dengan prinsip keadilan data, yang mewajibkan proses pentadbiran maklumat melalui standard etika dan ketelusan yang boleh diteliti oleh pelbagai pihak, termasuk masyarakat awam (Dencik, Hintz & Redden, 2019). Apabila keputusan untuk mengecualikan agensi atau meluluskan permintaan data dibiarkan dalam ruang eksklusif menteri atau jawatankuasa tertutup, data Kerajaan yang secara prinsipnya dimiliki oleh rakyat, berisiko digunakan untuk tujuan yang tidak diketahui atau tidak disepakati secara sosial (Tisne, 2020; Zuboff, 2019).

Selain itu, kajian oleh OECD (2021) menunjukkan bahawa ketelusan dalam pentadbiran data awam, termasuk melalui audit dan pelaporan berkala, berkait langsung dengan tahap kepercayaan rakyat terhadap institusi negara. Negara-negara seperti Estonia dan Denmark yang menginstitusikan "*public data dashboards*" dan pelaporan akses oleh pihak berkuasa menunjukkan kadar kepatuhan data yang lebih tinggi serta pengurangan risiko salah guna maklumat (UNESCO, 2022).

Oleh yang demikian, dicadangkan agar Seksyen 27 Akta 864 dipinda untuk mewajibkan pelaporan berkala kepada Jawatankuasa Kira-Kira Wang Negara (PAC) atau Jawatankuasa Pilihan Khas Parlimen bagi Komunikasi dan Digital (JKICT). Setiap pengecualian, permintaan data strategik, dan keputusan yang

memberi implikasi terhadap struktur maklumat negara perlu dilaporkan, direkod, dan boleh diaudit oleh entiti luar kerajaan. Penubuhan satu Jawatankuasa Audit Digital Negara (JADN) yang bersifat bebas dan rentas kepakaran dengan melibatkan ahli akademik, wakil masyarakat sivil, dan profesional teknologi juga wajar dipertimbangkan.

Fungsi jawatankuasa ini adalah untuk:

1. Menyemak semua permintaan dan pengecualian yang melebihi tahap risiko tertentu.
2. Mengaudit sistem kawalan dan penggunaan data secara berkala.
3. Menerbitkan laporan awam tahunan berkenaan status perkongsian dan pengurusan data kerajaan.

Sebagaimana dinyatakan oleh Milan dan Treré (2019), pembinaan kuasa digital yang lestari memerlukan kewujudan struktur kuasa yang dapat dinilai dan dicabar secara sah. Dalam erti kata lain, audit dan pelaporan bukan sekadar proses teknikal, tetapi merupakan bentuk perlindungan institusi terhadap kemungkinan penyelewengan maklumat dalam sistem yang sangat kompleks dan tidak kelihatan (Veale, Van Kleek & Binns, 2018).

Mekanisme semak dan imbang yang sah dan terbuka juga memberi kesan limpahan kepada pembinaan legitimasi awam terhadap sistem digital negara. Dalam jangka panjang, legitimasi inilah yang akan menentukan keberkesanan, keberterimaan, dan kebolehlestarian sistem perkongsian data nasional sebagai sebahagian daripada ekosistem kuasa negara yang sah dan berprinsip (Floridi, 2020; Souter, 2020).

6.4 Perlindungan hak data rakyat dan prinsip persetujuan bermaklum

Pengumpulan data besar-besaran oleh kerajaan dan sektor swasta, persetujuan bermaklum telah menjadi prinsip asas dalam ekosistem tadbir urus data demokratik (Sax, Helberger, & Bol, 2020). Namun, dalam konteks Akta 864, tiada peruntukan yang jelas atau wajib yang memperuntukkan keperluan mendapatkan persetujuan daripada pemilik data sebelum maklumat peribadi dikongsi antara agensi sektor awam. Hal ini menimbulkan persoalan mendalam mengenai kedudukan rakyat sebagai subjek data, adakah mereka memiliki kuasa terhadap informasi tentang diri mereka, atau sekadar objek yang digunakan untuk pemprosesan dasar?

Persetujuan bermaklum bukan sekadar proses formal, tetapi merupakan bentuk pengiktirafan ke atas maruah dan otonomi individu dalam ruang digital. Tanpa mekanisma untuk rakyat mengetahui, mengawal atau menolak penggunaan data peribadi mereka, sistem digital akan beralih daripada alat pengkhidmatan kepada alat pengawasan tersembunyi (Greenleaf & Waters, 2014). Prinsip *privacy by design* seperti yang dianjurkan dalam GDPR menuntut agar sebarang sistem pengendalian data wajib menyediakan lapisan perlindungan privasi secara sistematik dan bukannya sekadar bersifat reaktif atau selepas kejadian (Cavoukian, 2009).

Bahkan dalam negara-negara membangun seperti Brazil melalui *Lei Geral de Proteção de Dados* (LGPD), pengguna memiliki hak eksplisit untuk mendapatkan maklumat tentang tujuan, jangka masa penyimpanan, dan akses data mereka, serta berhak menarik balik persetujuan bila-bila masa (Doneda & Monteiro, 2021). Di Kenya, *Data Protection Act 2019* memperkenalkan hak kepada warga untuk menolak pemprosesan automatik data mereka jika ia memberi kesan besar kepada kehidupan individu (Makulilo, 2020). Namun, Akta 864 tidak memberikan sebarang bentuk hak yang setara kepada rakyat Malaysia dalam konteks sektor awam.

Tambahan pula, dalam seksyen-seksyen yang memperuntukkan perkongsian kepada pihak ketiga (Seksyen 17), persetujuan yang disebut hanya melibatkan persetujuan antara agensi, dan bukannya daripada subjek data itu sendiri. Ini bermaksud bahawa seseorang individu tidak mengetahui bila data peribadinya disalurkan ke agensi lain, untuk tujuan apa, dan siapa yang mengaksesnya. Ketelusan sebegini merupakan pelanggaran terhadap prinsip data subject empowerment yang menekankan bahawa subjek data mesti dilengkapi dengan informasi yang relevan dan diberi pilihan yang bermakna (Mantelero, 2016; Solove, 2013).

Hak data juga bukan semata-mata soal privasi, tetapi hak terhadap autonomi maklumat iaitu keupayaan individu untuk membina naratif, identiti dan keputusan berdasarkan maklumat tentang dirinya sendiri (Kerry, 2021). Tanpa jaminan bahawa data peribadi tidak akan digunakan secara manipulatif atau diskriminatif,

konsep kepercayaan sosial terhadap sistem digital akan terkikis, sebagaimana yang berlaku dalam kes penyalahgunaan data pendidikan di UK dan data kesihatan di Australia (Gellert, 2020; Jasanoff, 2004).

Oleh itu, dicadangkan agar Akta 864 diperkukuh dengan klausa Hak Data Rakyat, termasuk:

1. Kewajipan notifikasi awal kepada individu apabila data mereka diproses atau dikongsi;
2. Hak untuk mendapatkan penjelasan tentang tujuan dan entiti penerima data;
3. Pilihan untuk opt-out bagi tujuan bukan keselamatan atau darurat;
4. Kewujudan data ombudsman sebagai penjaga keadilan maklumat.

Sebagaimana ditegaskan oleh Hintz, Dencik dan Wahl-Jorgensen (2019), pembinaan sistem maklumat negara mesti dimulakan dari bawah. Daripada rakyat sebagai pemilik maklumat, bukan sekadar penerima dasar. Dalam kerangka negara yang berdaulat, kedaulatan maklumat tidak dapat dipisahkan daripada kedaulatan rakyat atas data dirinya sendiri.

6.5 Pelaksanaan laporan tahunan perkongsian data dan keterbukaan akses awam

Dalam struktur kuasa berasaskan maklumat, pelaporan tahunan bukan sekadar dokumentasi, ia adalah instrumen kawalan sosial terhadap sistem yang tidak kelihatan. Akta 864 telah pun memperuntukkan di bawah Seksyen 21 bahawa agensi sektor awam perlu menyediakan laporan bertulis kepada Ketua Pengarah mengenai butiran permintaan, maklum balas, dan alasan penolakan dalam proses perkongsian data. Namun, kelemahan ketara peruntukan ini ialah sifat tertutup pelaporan tersebut, hanya bersifat dalaman, tanpa sebarang keperluan untuk penerbitan awam atau semakan Parlimen.

Dalam demokrasi digital moden, kewajipan untuk melaporkan perlu diperluas kepada pelibatan awam sebagai sebahagian daripada sistem *"accountability by disclosure*" (Fung, Graham, & Weil, 2007). Laporan tahunan tentang perkongsian data harus diterbitkan secara umum, dengan struktur standard yang menyenaraikan jumlah permintaan, kelulusan, penolakan, agensi terlibat, dan kategori data yang dikongsi tanpa mendedahkan maklumat sensitif. Model sebegini telah dilaksanakan dalam *Open Data Reports* di United Kingdom, serta *Data Access Transparency Reports* di Australia, yang menyumbang kepada peningkatan kepercayaan rakyat terhadap sistem digital kerajaan (OECD, 2020; Gruen et al., 2014).

Lebih kritikal, laporan ini perlu diserahkan kepada Parlimen dan boleh diteliti oleh Jawatankuasa Pilihan Khas berkenaan komunikasi atau digital. Amalan ini bukan baharu, misalnya di Kanada, pelaporan tahunan di bawah Privacy Act diwajibkan untuk dibentangkan ke Parlimen, sementara dalam *Freedom of Information Act (FOIA) Amerika Syarikat*, agensi wajib memfailkan rekod tahunan akses maklumat yang kemudian dikompilasi oleh Jabatan Kehakiman dan dibuka kepada umum (Bannister & Connolly, 2012).

Tanpa pelaporan terbuka, kuasa maklumat yang semakin tersentralisasi akan kehilangan elemen legitimasi dan boleh menjurus kepada penyalahgunaan, seperti ditunjukkan dalam kes-kes kebocoran data rakyat di pelbagai negara (Gellert, 2020). Selain itu, laporan tahunan yang bersifat terbuka dapat menjadi bahan rujukan akademik, sivil dan industri untuk memahami pola penggunaan data awam, mengenal pasti trend risiko, dan mencadangkan reformasi proaktif berdasarkan data empirikal (Ruijer et al., 2017).

Dicadangkan agar Akta 864 dipinda bagi mewajibkan dua bentuk laporan:

1. Laporan Tahunan kepada Parlimen – Mengandungi butiran makro seperti bilangan permintaan data, kadar kelulusan, dan penilaian risiko tahunan.
2. Laporan Umum Akses Terbuka (*Public Data Transparency Report*) – Laporan ringkas berformat infografik, diterbitkan dalam portal awam seperti MyGOV, dan dibentangkan dalam bahasa awam.

Keterbukaan ini juga seiring dengan prinsip open government yang telah diiktiraf dalam pelbagai platform antarabangsa seperti *Open Government Partnership (OGP)* dan *United Nations E-Government Survey*, di mana keterbukaan maklumat dinilai sebagai indikator prestasi tadbir urus data negara (UN DESA, 2022). Dalam hal ini, Malaysia harus bergerak ke arah struktur pelaporan yang bersifat proaktif, responsif dan merakyatkan data—kerana dalam masyarakat bermaklumat, siapa yang berkongsi dan siapa yang mengetahui adalah sebahagian daripada siapa yang memegang kuasa.

6.6 Pembangunan kod tadbir urus data nasional berteraskan nilai tempatan

Sebuah negara tidak dibina hanya atas kekuatan ekonomi dan struktur undang-undang, tetapi atas kesepakatan nilai dan legitimasi budaya yang menyuburkan keadilan dan amanah. Dalam konteks data, hal ini lebih mendesak. Tanpa nilai, data hanyalah instrumen pengumpulan. Tanpa panduan etika yang tertanam dalam kebijaksanaan lokal, sistem tadbir urus akan tunduk kepada struktur teknokratik yang mudah dimanipulasi oleh kuasa luar. Maka, pembangunan sebuah Kod Tadbir Urus Data Nasional yang berpaksikan nilai tempatan bukan sekadar keperluan polisi, tetapi tuntutan peradaban.

Pengalaman negara-negara global menunjukkan bahawa keberkesanan tadbir urus data bergantung bukan sahaja kepada kerangka perundangan, tetapi kepada nilai teras yang mendasarinya. Di Aotearoa New Zealand, pendekatan *Te Mana Raraunga* meletakkan prinsip Maori data sovereignty sebagai asas kepada semua polisi pengurusan data, berteraskan kedaulatan spiritual, komuniti dan naratif warisan (Kukutai & Taylor, 2016). Di Kanada, *OCAP Principles* oleh komuniti *First Nations* menetapkan bahawa data mesti dikawal oleh komuniti itu sendiri atas dasar *ownership, control, access, and possession* (FNIGC, 2014). Ini menunjukkan bahawa struktur yang berkesan tidak muncul dari salinan model Barat, tetapi daripada ijtihad lokal terhadap realiti sosial, moral dan identiti kolektif.

Dalam konteks Malaysia, kod ini wajar memikul peranan ganda: sebagai pelindung data strategik dan sebagai refleksi nilai nasional. Ia perlu menjawab soalan-soalan kritikal: Siapa yang menentukan nilai data? Atas dasar apa data dikongsi? Apa bentuk kemaslahatan yang sah? Oleh itu, kod ini perlu menggabungkan prinsip maqasid syariah (maslahat, amanah, keadilan), falsafah adat Melayu (tatasusila, kepemimpinan beradab), dan pendekatan tadbir urus kontemporari (*risk-informed, ethical design*).

Elemen utama kod ini boleh dirangka seperti berikut:

1. Deklarasi Nilai Teras – merangkumi tanggungjawab kolektif (mas'uliyyah), kesaksamaan data (*justice in access*), dan nilai ruhani sebagai asas kepemilikan maklumat.
2. Kategori Data Warisan – seperti data wakaf, silsilah, bio-kepelbagaian, adat minoriti dan sistem keilmuan tempatan, yang tidak boleh diurus seperti data pentadbiran biasa (Prinsloo, 2022).
3. Kerahsiaan Bermakna dan Hak Asasi Maklumat – mengimbangi antara perlindungan privasi dan hak rakyat untuk mengetahui apa yang dikumpulkan tentang mereka (Floridi, 2020; Hummel et al., 2021b).
4. Pemuridan Tadbir Urus (*Data Stewardship*) – kod ini harus menetapkan bahawa kerajaan bukan pemilik mutlak data, tetapi murabbi yang memfasilitasi tadbir urus bersama antara sektor awam, masyarakat sivil, dan institusi komuniti (Couldry & Mejias, 2019).
5. Standard Penafsiran Kontekstual – menghindari *absolutisme* legalistik. Misalnya, konsep "data sensitif" tidak hanya ditentukan oleh kategori teknikal, tetapi oleh sensitiviti budaya dan kesan terhadap struktur sosial.

Dalam konteks Akta 864, kod ini perlu berfungsi sebagai lapisan "takwil nilai" (*value exegesis*) kepada seksyen-seksyen berkaitan perkongsian, pengecualian, dan perlindungan data strategik. Ini bukan soal menambah birokrasi, tetapi menghidupkan kerangka undang-undang agar berjiwa dan berprinsip. Kod ini juga boleh digubal melalui badan antara agensi yang melibatkan institusi fatwa, DBP, akademia, masyarakat adat dan digital ethnographers, agar perdebatan tidak dimonopoli oleh pakar teknikal semata-mata.

Akhirnya, kod ini adalah bentuk perlembagaan kecil data yang menjadi rujukan moral dan dasar dalam semua keputusan strategik negara yang melibatkan data. Ia bukan hanya melindungi maklumat, tetapi melindungi makna; bukan hanya menjamin keselamatan siber, tetapi membentuk etika digital nasional. Hanya dengan kerangka seperti ini, Malaysia boleh berdiri sebagai negara digital yang bukan sekadar canggih, tetapi berdaulat dalam erti sebenar yang merangkumi kuasa, nilai, dan maruah.

7.0 Kesimpulan

Data bukan lagi sekadar aset digital, ia telah menjadi medan kuasa yang menentukan siapa yang mentadbir, siapa yang dipantau, dan siapa yang dipinggirkan. Dalam landskap global yang semakin dikawal oleh kuasa platform dan piawaian teknokratik antarabangsa, Malaysia berdepan risiko menjadi pengguna data tanpa

kedudukan strategik dalam sistem yang ia sendiri sedang bina. Akta 864 muncul dalam saat yang kritikal: ia berpotensi menjadi titik mula pembentukan ekosistem maklumat nasional yang tersusun dan berfungsi. Namun, tanpa prinsip kedaulatan yang jelas, akta ini juga boleh menjadi pintu belakang kepada ketirisan kuasa, penjajahan algoritma, dan pelucutan legitimasi digital negara.

Analisis ini menunjukkan bahawa kelemahan struktur dalam Akta 864 bukan sahaja bersifat teknikal, tetapi menjejaskan asas kuasa nasional secara langsung. Ketidaktentuan dalam takrifan data strategik, ketiadaan klausa penyimpanan berdaulat, kuasa pengecualian menteri tanpa semak dan imbang, serta tiadanya perlindungan terhadap hak data rakyat, semuanya membentuk satu landskap yang rapuh untuk negara yang bercita-cita menjadi hab data serantau. Lebih daripada itu, ketiadaan satu kod nilai dalam tadbir urus data menjadikan sistem digital Malaysia terdedah kepada logik universal yang tidak selalu sesuai dengan realiti budaya, sejarah, dan falsafah negara.

Cadangan-cadangan penambahbaikan yang dikemukakan; Dari pewartaan data strategik hingga pembentukan kod tadbir urus berteraskan nilai tempatan bukan sekadar intervensi dasar. Ia adalah usaha membina kembali kedudukan rakyat, negara dan maklumat dalam satu ekosistem yang adil, berdaya tahan, dan berdaulat. Dalam dunia maklumat, yang mengawal data bukan sahaja mengawal infrastruktur, tetapi mengawal naratif, keputusan, dan masa depan.

Malaysia memerlukan bukan hanya dasar yang canggih, tetapi prinsip yang kukuh; bukan sekadar sistem yang efisien, tetapi sistem yang membimbing. Di sinilah letaknya nilai sebenar kedaulatan data, bukan pada jumlah data yang dimiliki, tetapi pada kuasa untuk mentafsirnya dengan adil, mengawalnya dengan berani, dan menggunakannya untuk membina bangsa yang merdeka.

Penghargaan

Penulis ingin merakamkan setinggi-tinggi penghargaan kepada Encik Mohd Zul Fahmi Md Bahrudin dan Encik Mohd Asyraf Mohd Farique dari IRIS Institute, serta Encik Muhammad Thalhah Kamarol Zaman, Penasihat Ekonomi di *Department for Science, Innovation and Technology*, Kerajaan *United Kingdom* atas penglibatan mereka dalam beberapa siri diskusi intelektual yang telah memberi sumbangan besar terhadap pembentukan kedalaman konseptual dan hala tuju strategik penulisan ini. Pandangan-pandangan kritikal yang dikongsikan oleh mereka, yang merangkumi pelbagai disiplin dan berakar daripada pengalaman dalam dasar serta geopolitik digital, telah membantu memperhalusi hujah-hujah utama berkenaan isu kedaulatan data, struktur tadbir urus, dan autonomi digital negara. Diskusi-diskusi tersebut telah menjadi pencetus kepada pemerkasaan kerangka analisis dan penilaian terhadap struktur Akta Perkongsian Data 2025. Segala dapatan, tafsiran dan sebarang kekhilafan dalam artikel ini bagaimanapun adalah tanggungjawab penuh penulis.

Rujukan

Arun, C. (2019). AI and the Global South: Designing for other worlds. In M. Dubber, F. Pasquale, & S. Das (Eds.), The Oxford Handbook of Ethics of AI. Oxford University Press.

al-Ghazali. (1985). Nasihat al-Muluk (The Book of Counsel for Kings). OUP.

al-Raysuni, A. (2006). Imam al-Shatibi's Theory of the Higher Objectives and Intents of Islamic Law. IIIT.

APEC. (2015). Privacy Framework. Asia-Pacific Economic Cooperation.

Auda, J. (2008). Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach. International Institute of Islamic Thought.

Bannister, F., & Connolly, R. (2012). Defining e-Governance. Government Information Quarterly, 29(1), 1–10.

Barocas, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. Proceedings of the Engaging Data Forum.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2022). Digital Business Strategy and Value Creation. MIS Quarterly.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. International Journal of Law and Information Technology, 19(3), 187–223.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information & Privacy Commissioner of Ontario.

Chander, A., & Le, U. P. (2014). Data nationalism. Emory Law Journal, 64(3), 677–739.

Chenou, J.-M., & Cepeda-Másmela, C. (2019). Digital Rights and the Global South: Infrastructures of Control and Resistance. Telecommunications Policy, 43(10).

Chilisa, B. (2017). Indigenous Research Methodologies. SAGE Publications.

Couldry, N., & Mejias, U. A. (2019). The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford University Press.

De Filippi, P., & Greenstein, S. (2020). Data Localization and Governance: Economic and Legal Perspectives. Harvard Business School Working Paper.

Dehghani, Z. (2020). Data Mesh: Delivering Data-Driven Value at Scale. ThoughtWorks.

DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.

Dencik, L., Hintz, A., & Redden, J. (2019). Data Justice: Towards a Political Economy of Datafication. Policy Press.

Doneda, D., & Monteiro, M. A. (2021). The Brazilian General Data Protection Law (LGPD). International Data Privacy Law, 11(2), 132–145.

Elasha, M. (2021). Digital Sovereignty in the Muslim World: A Lost Narrative. Islam21C.

European Commission. (2020a). A European Strategy for Data.

European Commission. (2020b). Proposal for a Regulation on European Data Governance (Data Governance Act).

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378.

FNIGC. (2014). The First Nations Principles of OCAP. First Nations Information Governance Centre.

Fricker, M. (2007). Epistemic Injustice: Power and the Ethics of Knowing. Oxford University Press.

Fung, A., Graham, M., & Weil, D. (2007). Full Disclosure: The Perils and Promise of Transparency. Cambridge University Press.

GDPR. (2018). General Data Protection Regulation (EU) 2016/679.

Gellert, R. (2020). Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 10(1), 20–33.

Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws & many bills. Privacy Laws & Business International Report, 157.

Greenleaf, G., & Waters, N. (2014). Global Data Privacy Laws 2013: eighty-nine countries, and accelerating. Privacy Laws & Business International Report, (123), 10–13.

Gruen, N., Houghton, J., & Tooth, R. (2014). Open for Business: How Open Data Can Help Achieve the G20 Growth Target. Lateral Economics.

Gurumurthy, A., & Chami, N. (2020a). Data Sovereignty and the Digital Economy: Building Democratic Infrastructure. IT for Change.

Gurumurthy, A., & Chami, N. (2020b). Towards a digital new deal: Civil society position on data and digital intelligence. IT for Change.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). Digital Citizenship in a Datafied Society. Polity Press.

Hummel, P., Braun, M., & Dabrock, P. (2021a). Data sovereignty: A review. Big Data & Society, 8(1).

Hummel, P., Braun, M., & Dabrock, P. (2021b). Sovereignty and Data Ethics: Understanding the Tension.

Big Data & Society, 8(2).

Ibn Khaldun. (1967). The Muqaddimah: An Introduction to History (trans. F. Rosenthal). Princeton University Press.

ICO. (2023). Information Commissioner's Annual Report and Financial Statements 2022–23.

Jasanoff, S. (2004). States of Knowledge: The Co-production of Science and Social Order. Routledge.

Kerry, C. F. (2021). Why Data Ownership is the Wrong Approach to Protecting Privacy. Brookings Institution.

Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. Penguin Press.

Kukutai, T., & Taylor, J. (2016). Indigenous Data Sovereignty: Toward an Agenda. ANU Press.

Kuner, C. (2015a). Data sovereignty and the cloud – A global perspective. Journal of International Data Privacy Law, 5(4), 221–226.

Kuner, C. (2015b). Transborder Data Flows and Data Privacy Law. Oxford University Press.

Makulilo, A. B. (2020). African Data Protection Laws: A Comparative Analysis. Springer.

MAMPU. (2022). Laporan Pelaksanaan Projek Perkongsian Data Sektor Awam Fasa II. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU).

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer Law & Security Review, 32(2), 238–255.

Mehta, P. (2023). India's Digital Personal Data Protection Act: Structure, Risks and Opportunities. Observer Research Foundation.

Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond data universalism. Television & New Media, 20(4), 319–335.

Milner, A. (2002). The Malays. Wiley-Blackwell.

Morozov, E. (2011). The Net Delusion: The Dark Side of Internet Freedom. PublicAffairs.

MyDigital. (2021). Malaysia Digital Economy Blueprint. Economic Planning Unit, Prime Minister's Department. https://www.epu.gov.my/en/digital-economy-blueprint

OECD. (2020). The Path to Becoming a Data-Driven Public Sector. OECD Digital Government Studies.

OECD. (2021). Data Governance for Growth and Well-being. OECD Digital Economy Paper No. 308.

OECD. (2022). Data Governance for Growth and Well-Being. OECD Publishing.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4).

Prinsloo, P. (2022). Reimagining Data Governance: A Humanising Perspective. International Review of Information Ethics.

Quijano, A. (2000). Coloniality of power, Eurocentrism, and Latin America. International Sociology, 15(2), 215–232.

Ruijer, E., Grimmelikhuijsen, S., & Meijer, A. (2017). Open Data for Democracy: Developing a Theoretical Framework for Open Data Use. Government Information Quarterly, 34(1), 45–52.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. Big Data & Society, 6(1), 1–12.

Sardar, Z. (2003). Islamic Futures: The Shape of Ideas to Come. Mansell Publishing.

Sax, M., Helberger, N., & Bol, N. (2020). Health as a Means Towards Profitable Ends: The Politics of Health. Health Policy and Technology, 9(1), 88–98.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.

Souter, D. (2020). Data sovereignty and digital development: Challenges and prospects. Association for Progressive Communications.

Swire, P., & Hemmings, D. (2019). The CLOUD Act: A Comprehensive Overview. Journal of National

Security Law & Policy, 10(1), 1–48.

Syed Muhammad Naquib al-Attas. (1978). Islam and Secularism. ABIM.

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751–752.

Taylor, L. (2021). Data justice and data solidarity. Information, Communication & Society, 24(6), 834–850.

Tikk, E., & Kerttunen, M. (2020). The sovereignty of cyberspace: Institutions and norms in digital governance. NATO CCDCOE.

Tisne, M. (2020). The Data Delusion: Protecting Individual Data Isn't Enough When the Harm is Collective. Stanford Cyber Policy Center.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(203).

UN DESA. (2022). United Nations E-Government Survey 2022: The Future of Digital Government. United Nations Department of Economic and Social Affairs.

UNCTAD. (2021). Digital Economy Report 2021: Cross-border Data Flows and Development.

UNDP. (2022). Digital Strategy 2022–2025.

UNESCO. (2022). Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives.

United Nations. (2022). Global Review of National Data Strategies. UNCTAD Digital Economy Report.

Veale, M., Van Kleek, M., & Binns, R. (2018). Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.

World Bank. (2021). World Development Report 2021: Data for Better Lives.

Wu, T. (2018). The Curse of Bigness: Antitrust in the New Gilded Age. Columbia Global Reports.

Zeng, J., Stevens, T., & Chen, Y. (2021). China’s solution to global data governance: Unpacking the “Data Security Law.” Internet Policy Review, 10(3).

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs.