p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

PRIVACY LAWS DI INDONESIA DI ERA REVOLUSI INDUSTRI 5.0

Hakki Fajriando
Badan Riset dan Inovasi Nasional
hakk001@brin.go.id

ABSTRAK

Tulisan ini berupaya mengkaji secara kritis kerangka tata kelola data pribadi di Indonesia dalam menghadapi era 5.0. Dampak Revolusi Industri 5.0 memerlukan adanya penyesuaian terhadap kerangka regulasi tata kelola data di Indonesia. Kerangka penetapan standar regulasi data yang berkembang di Amerika Serikat (*digital privacy laws*), Uni Eropa (GPDR), dan Tiongkok (PIPL) selama ini dianggap masih mengonseptualisasikan data sebagai sumber daya dan aset ekonomi yang menghasilkan pendapatan. Penelitian ini berargumen bahwa pemerintah Indonesia juga menerapkan metafora konsep "data sebagai sumber daya" dalam kerangka kebijakannya. Mengadopsi metafora konsep semacam ini melanggengkan dimensi ekonomi dari kolonialisme data, yang melibatkan pemerintah dan perusahaan-perusahaan teknologi besar yang mengambil keuntungan dengan mengekstraksi dan memonopoli data masyarakat, tidak jarang dengan melanggar hak privasi individu dan menimbulkan *societal harm* dan konsekuensi negatif terhadap demokrasi. Selain itu, Tulisan ini berargumentasi bahwa untuk memerangi kolonialisme data, penekanan Indonesia terhadap kedaulatan data tidak boleh hanya terfokus pada kedaulatan negara namun juga pada masyarakat yang menghasilkan data. Berfokus pada kedaulatan masyarakat atas datanya berarti memperhatikan karakteristik sosial data dan menjauhkan landasan kebijakan dari metafora konsep "data sebagai sumber daya". Terakhir, Pemerintah juga diharapkan dapat membangun otoritas PDP yang independen untuk membangun kepercayaan masyarakat terhadap perlindungan data pribadi dan mendorong akselerasi transformasi digital yang berkesinambungan. Revolusi Industri 5.0 juga menimbulkan kesadaran diperlukannya keseimbangan antara perlindungan privasi dan perdagangan digital yang efisien.

Kata Kunci: Revolusi Industri 5.0, Tata Kelola Data, Kolonialisme Data, Kedaulatan Data, Data sebagai Sumber Daya

I. PENDAHULUAN

Gagasan Revolusi Industri 5.0 terutama berkaitan dengan kemajuan yang sedang berlangsung dalam otomasi dan digitalisasi dalam sektor industri dan produksi (Calaghan, 2019). Penekanan utama dari gagasan ini adalah pada penggabungan teknologi dan elemen manusia (Costa et al., 2022). Revolusi Industri 5.0 lebih menekankan pada penggabungan teknologi mutakhir, termasuk kecerdasan buatan (AI), *Internet of Things* (IoT), dan robotika, dalam hubungannya dengan keahlian dan inovasi manusia. Integrasi ini bertujuan untuk mendorong kemajuan sistem produksi yang ditandai dengan peningkatan efisiensi, fleksibilitas, keberlanjutan, dan perbaikan kesejahteraan (George & George, 2020).

Revolusi Industri 5.0 memunculkan kesadaran akan potensi tantangan yang signifikan, termasuk dalam bidang hukum, dimana diperlukan langkah-langkah proaktif untuk mengidentifikasi dan mengatasi tantangan-tantangan ini. Perkembangan teknologi

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

yang pesat, seperti kecerdasan buatan, *Internet of Things*, dan *blockchain*, mempunyai dampak yang besar memerlukan pengaturan baru yang mengatur perlindungan data, privasi, dan *e-commerce*. Permasalahan privasi data menjadi salah satu perhatian utama di era Revoluasi Industri 5.0, dimana peraturan yang mengenai pengumpulan, penggunaan dan penyimpanan pelanggan data diramalkan akan semakin ketat. (Chen et al., 2012; Mehmodd, 2021). Salah satu isu sentral di era ini adalah semakin meningkat pertukaran data lintas batas yang luas. Hal ini menimbulkan kekhawatiran dalam hal privasi dan keamanan data pemerintah dan warga negara. Banyak orang khawatir informasi pribadi mereka dikumpulkan, ditransfer, dan digunakan tanpa sepengetahuan atau izin mereka.

Isu mengenai perlindungan data pribadi merupakan salah satu isu penting yang menjadi perhatian. Banyaknya penggunaan digital platform meningkatkan urgensi pengaturan mengenai perlindungan data pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. Dalam beberapa tahun terakhir, Indonesia mengalami berbagai insiden kebocoran data. Di tahun 2020 saja misalnya tercatat adanya kasus bocornya data pribadi pada 12.115.583 akun pengguna Tokopedia dan diperjual belikannya 1,2 juta catatan pengguna Bhineka.com. Kebocoran data 12.957.573 akun pengguna Bukalapak juga turut menjadi perhatian di tahun yang sama. Tahun 2021 mencatat terjadinya kebocoran data sekitar 1,3 juta data pengguna e-HAC yang dikelola Kemenkes serta data 279 juta pengguna BPJS. Sementara itu, pada tahun 2022 tercatat beberapa dugaan pembobolan pelanggaran data diajukan di Indihome hingga kasus PLN. Yang lebih menghebohkan adalah kemungkinan bocornya data 325 juta registrasi kartu SIM telepon yang diklaim dari Kementerian Komunikasi dan Informatika(Lesmana, Elis, Hamimah, 2022). Banyaknya kasus-kasus kebocoran data pribadi yang terjadi, menunjukkan bahwa hak atas privasi warga negara Indonesia sangat rentan untuk disalahgunakan.

Tata kelola data diperlukan karena "data dalam bentuk digital adalah [sic] "..secara rutin dibuat, dikumpulkan, dan dibagikan ke seluruh dunia untuk mendukung fungsi inti masyarakat, termasuk sistem kesehatan, transportasi, perdagangan internasional, dan keamanan nasional" (Arner *et al.*, 2021). Oleh karena itu, pemerintah menganggap data digital sebagai aset yang berharga. Alirannya harus diatur dengan cara yang menguntungkan warga dan perekonomiannya (Ciuriak, 2022). Dalam hal tata kelola digital global, secara umum terdapat dua kubu gaya tata kelola (Basu & Nachiappan, 2020). Yang pertama adalah Amerika Serikat. Rezim tata kelola data di Amerika Serikat secara umum dikenal sebagai *digital privacy laws* (Viljoen, 2020).. Prioritas utama tata kelola data di Amerika Serikat umumnya adalah untuk mengizinkan aliran data melintasi perbatasan dengan sesedikit mungkin intervensi, dengan tujuan untuk mempercepat inovasi Silicon Valley dan manfaat ekonomi dari hal tersebut. Uni Eropa, melalui General Data Protection Regulation (GPDR), berupaya memodifikasi pendekatan AS dengan menerapkannya peraturan mengenai perlindungan konsumen dan warga negara. Kubu kedua terdiri dari negara-negara dari BRICS dan *Global South*, yang menekankan kedaulatan data dan menolak kolonialisme data. Dalam pandangan kubu kedua pada intinya merumuskan kolonialisme data sebagai "gagasan yang dimiliki oleh perusahaan teknologi asing (yang sebagian besar berbasis di AS).menuai keuntungan dari data yang dihasilkan oleh warga negara-negara *Global South*" (Basu & Nachiappan,2020). Menurut Basu dkk. (2019), kedaulatan data mengacu pada hak kedaulatan setiap negara untuk mengatur data yang berasal dari dalam batas wilayahnya.

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

Sejalan dengan kolonialisme data, versi kedaulatan data ini memastikan bahwa data suatu negara tidak digunakan untuk keuntungan perusahaan swasta asing tetapi untuk meningkatkan pelayanan publik dalam negeri dan pertumbuhan ekonomi di negara-negara tersebut. Tiongkok adalah negara yang paling menonjol di kubu kedua. Tiongkok, melalui kebijakan terbarunya-*Personal Information Protection Law* (PIPL), menekankan konsep "internet otoriter, di mana teknologi pengawasan dan identifikasi membantu memastikan sosial kohesi dan keamanan" (O'Hara & Hall, 2018).

Perbedaan sikap dan prioritas pembuat standar global, seperti AS, UE, dan Tiongkok, inilah yang menyebabkan lanskap regulasi data secara global menjadi terfragmentasi (Arner dkk., 2021). Meskipun mereka pendekatan yang berbeda, para pembuat standar tersebut pada dasarnya memandang data sebagai sumber daya. Data juga berulang kali dibingkai sebagai "kekuatan alam yang harus dikendalikan dan sebagai sumber daya yang harus dikonsumsi" (Puschmann & Burgess, 2014). Metafora data seperti ini sangat penting karena mempengaruhi kesadaran publik, kebijakan, tata kelola, desain teknologi, dan model bisnis (Sinha & Basu, 2021). Pemikiran tentang data sebagai sumber daya membingkainya sebagai sesuatu yang dapat "diekstraksi, disempurnakan, dinilai, dibeli, dan dijual dengan cara yang berbeda" (*The Economist*, 2017). Dengan kata lain, data dianggap sebagai sesuatu " sederhananya berada 'di depan mata', siap untuk diperebutkan dan siap untuk ditambang" (Kovacs & Ranganathan, 2019). Data juga dianggap sebagai aset yang menghasilkan pendapatan, yang merupakan ekstensi dari konseptualisasinya sebagai sumber daya (Birch et al., 2021).

Tulisan ini berargumentasi bahwa pendirian Indonesia saat ini mengenai tata kelola data lebih menekankan pada 'data sebagai sumber daya'. pola pikir yang telah diadopsi oleh pembuat standar di bidang ini, seperti AS, UE, dan Tiongkok. Pola pikir ini melanggengkan kolonialisme data perusahaan teknologi atas data masyarakat. Tulisan itu berpendapat bahwa ada kebutuhan untuk beralih ke perhatian terhadap karakteristik sosial data. Tulisan ini berpendapat bahwa untuk memerangi kolonialisme data, penekanan konsep kedaulatan data tidak boleh hanya fokus pada kedaulatan negara, namun juga pada masyarakat yang menghasilkan data.

II. METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan penelitian hukum normatif yang difokuskan pada tinjauan pustaka untuk mengumpulkan informasi dari berbagai literatur tentang topik hukum yang dipelajari. Penelitian hukum normatif cenderung mewujudkan hukum sebagai perspektif disiplin, memandang hukum hanya dari perspektif norma yang bersumber dari masalah-masalah sosial. Oleh karena itu, penelitian ini menggunakan metode normatif untuk mengkaji norma hukum yang terkandung dalam muatan RUU Perlindungan Data Pribadi, yang digunakan sebagai solusi atas permasalahan yang timbul di masyarakat terkait perlindungan data pribadi.

III. HASIL DAN PEMBAHASAN: KERANGKA PERLINDUNGAN DATA PRIBADI DI INDONESIA-ANTARA DATA SEBAGAI *CAPITAL RESOURCES* DAN DATA SEBAGAI *SOCIAL LABOUR*

Konsep data sebagai sumber daya modal (*data as capital resources*) memahami data sebagai sebuah sampah konsumsi digital yang tidak memiliki kegunaan, namun mengalami proses daur ulang oleh perusahaan *platform* digital untuk mendapatkan

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

angka ekonomi yang tinggi. (Sudibyo, 2019). Julie E. Cohen menelusuri bagaimana perusahaan platform seperti Amazon dan Facebook mengamankan *quasi-ownership* terhadap data pengguna melalui "*enclosure of data*" dan mengidentifikasi pemrosesan informasi dalam "*data refineries*" sebagai "alat produksi ekonomi yang teramat penting (Cohen, 2019)". Sementara itu, Shoshanna Zuboff membandingkan proses produksi data dengan bentuk-bentuk akumulasi kekayaan berbasis penaklukan (*conquest-based wealth accumulation*), yang menyamakan kehidupan privat masyarakat dengan benua Asia, Afrika, dan Amerika prakolonial, yang diserbu dan dijarah demi keuntungan oleh perusahaan-perusahaan teknologi (Zuboff & Schwandt, 2019). Couldry & Mejias (2018) menekankan bahwa hegemoni *big tech companies*, baik asing atau "pribumi", dalam menggunakan, menyimpan, dan mengambil keuntungan dari data yang diambil dari warga negara sebagai bentuk kolonialisasi. Alasan mendasar yang memungkinkan terjadinya hegemoni semacam ini adalah pandangan bahwa data merupaka "sumber daya" yang berada di depan mata dan menunggu untuk diekstraksi dan dieksploitasi. Pemikiran semacam ini mengingatkan pada prinsip *terra nullius* yang digunakan oleh penjajah dari barat, yang mengonsepkan bahwa tanah yang tidak dimiliki oleh siapa pun dapat secara sah diduduki, dimiliki, dan dieksploitasi oleh entitas privat atau negara mana pun.

Tata kelola data pribadi berdasarkan konsep data sebagai modal/sumber daya banyak dikritik karena dianggap gagal mengamankan otonomi individu manusia sebagai subjek data dan dengan demikian menghambat realisasi manfaat privasi terhadap individu dan masyarakat. Rezim *privacy laws* berdasarkan pemberitahuan dan persetujuan (*notice-and-consent regime*) dianggap gagal menjamin bahwa masyarakat untuk mengontrol dan mengakses data pribadi mereka. Individu secara umum hampir tidak pernah membaca kebijakan privasi yang mereka setujui dan tidak punya cara untuk menawar ketentuan yang ada di dalamnya (Obar dan Oeldorf-Hirsch, 2020). Data pribadi yang diperoleh melalui produksi data juga dianggap tidak dapat dimusnahkan (*nonextinguishable*), dan dapat digunakan kembali (*reusable*), yang artinya aliran data dan cara penggunaannya dapat berubah seiring berkembangnya teknologi dan model bisnis (Richards dan Hartzog, 2019).

Kritik terhadap konsep data sebagai sumber daya/modal pada gilirannya melahirkan pemikiran yang menekankan aspek sosial dari data, dimana privasi dianggap memiliki posisi penting dalam pembinaan kondisi kewarganegaraan publik dan pemerintahan publik. Priscilla M. Regan, misalnya, berargumentasi bahwa privasi penting secara sosial karena privasi memfasilitasi berkembangnya politik demokratis melalui perlindungan kebebasan berserikat dan kebebasan berpendapat (Regan, 1995). Aliran pemikiran ini berpendapat bahwa terdapat *social value* ketika individu diberikan kapasitas mereka untuk mengembangkan *self-knowledge* dan bertindak sesuai dengan pengetahuan tersebur (yang diamankan dengan perlindungan privasi yang kuat). Contohnya adalah kenyataan bahwa demokrasi yang berkembang membutuhkan individu yang berpengetahuan (*knowledgeable*) dan memiliki kemampuan melakukan kehendak mereka sendiri (*own free will*). Sederhananya, kita tidak bisa memiliki demokrasi tanpa warga negara yang bertindak secara otonom.

Hal ini sejalan dengan konsep data sebagai hasil kerja manusia (*data as social labour*). Konsep *data as social labour* adalah sebuah konsep yang mendudukan data yang didapat dari perilaku pengguna internet sebagai hak miliknya sendiri. Alhasil, konsep ini jika dimanfaatkan dengan baik harusnya dapat memberikan keuntungan bagi

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

pengguna internet itu sendiri. Perspektif *data as social labour* beranggapan bahwa data itu seyogyanya dikembalikan kepada pengguna (individu) masing-masing, tanpa melihat dari apa dan bagaimana pemanfaatan data itu seterusnya. Dalam hal ini perspektif *data as social labour* merepresentasikan pentingnya pengembangan kapabilitas warga negara dalam proses Pembangunan (Sudibyo, 2019).

Sebelum diundangkannya UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP), secara umum, aturan berkaitan dengan perlindungan data pribadi di Indonesia termaktub dalam beberapa peraturan perundangundangan yang terpisah dan hanya menggambarkan konsep perlindungan data pribadi secara umum dan aturan yang hanya dituangkan dalam bentuk Peraturan Menteri Komunikasi dan Informatika Republik Indonesia. Beberapa aturan Undang-undang yang terpisah tersebut antara lain Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dalam Pasal 28 G yang memuat norma tentang perlindungan data pribadi, Undang-Undang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008, Undang-Undang Nomor 43 Tahun 2009, tentang Kearsipan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas UndangUndang Nomor 7 Tahun 1992 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), dan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Pengesahan UU PDP pada tahun 2022 memberikan kerangka kerja yang khusus dan komprehensif dalam penanganan serta perlindungan data pribadi di Indonesia. Regulasi ini diharapkan dapat memperkuat kesiapan negara dalam melindungi data pribadi warganya. Selain itu, UU ini juga dirancang untuk memberikan jaminan rasa aman kepada individu terhadap data pribadi mereka. Lebih lanjut, regulasi ini memiliki peran penting dalam menjerat pelaku penyalahgunaan data pribadi dengan sanksi yang tegas, sehingga memberikan dasar hukum yang kokoh untuk menjaga integritas dan keamanan data pribadi (Ravlindo & Gunadi, 2022).

Namun, sayangnya di dalam Undang-Undang Nomor 27 Tahun 2022 Perlindungan Data Pribadi belum ada dimuat aturan mengenai adanya lembaga pengawas independen untuk melakukan pengawasan perlindungan data. Dijelaskan pada Undang-Undang Perlindungan Data Pribadi di Pasal 58, akan terdapat suatu lembaga yang dibentuk dan ditugaskan oleh Presiden sebagai kepala pemerintah Lembaga otoritas ini juga akan betanggungjawab kepada Presiden sebagai Kepala Negara, yang bernama Lembaga Otoritas Perlindungan Data Pribadi atau LOPDP. Lembag otoritas tersebut ditugaskan untuk melindungi data pribadi warga negara Indonesia dan menjalankan amanat yang tertuang pada Undang-Undang Data Pribadi. Perlunya lembaga pengawas untuk mencegah konflik kepentingan, pengendali data tidak hanya lembaga privat. Ketiadaan lembaga independen bisa dianggap Indonesia tidak memenuhi syarat *adequate level of protection*. Analisis terhada Undang-undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (PDP) menunjukkan bahwa kementerian dan lembaga di Indonesia menjalani dua peranan, yaitu sebagai entitas yang turut mengatur dan mengimplementasikan isu PDP sekaligus sebagai pelaku pemrosesan data pribadi. Padahal Indonesia sesungguhnya memerlukan Otoritas Pengawas Pelindungan Data Pribadi (Otoritas PDP) yang memiliki kompetensi sekaligus bisa secara adil melaksanakan tugas dan kekuasaannya untuk mengawasi

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

kegiatan pemrosesan data yang dilakukan termasuk oleh atau untuk sektor publik. Lembaga otoritas perlindungan data pribadi perlu memiliki indepedensi atau kemandirian dalam menjalankan tugas dan amanat dari Undang-Undang Perlindungan Data Pribadi, agar terciptanya *fairness* atau keadilan pada saat penegakkan Undang-Undang Perlindungan Data Pribadi tersebut, khususnya untuk menjamin bahwa pemerintah tidak dilindungi pada saat pihak pemerintah melanggar peraturan yan termuat dalam Undang-Undang Perlindungan Data Pribadi. Sejauh ini, UU PDP belum dapat menghadirkan Otoritas PDP yang independen. Kewenangan utama penyelenggaraan pelindungan data pribadi dan pengawasannya ada pada pemerintah (Pasal 58 ayat (1) UU PDP)," Dalam UU PDP, pemerintah menurunkan otoritasnya pada sebuah "lembaga" yang nantinya akan ditetapkan oleh presiden (Pasal 58 ayat (2) dan (3) UU PDP) dan lembaga tersebut juga akan bertanggung jawab kepada presiden (Pasal 58 ayat (4) UU PDP). Nampak bahwa bakal Otoritas PDP di Indonesia adalah sebuah lembaga yang berada pada kaki pemerintah. Sehingga, pemerintah akan memiliki 2 (dua) persona, yaitu sebagai pengawas sekaligus yang diawasi. Tanpa otoritas PDP yang independen, Indonesia akan mengalami kesulitan di dalam membangun kepercayaan masyarakat dan mendorong akselerasi transformasi digital yang berkesinambungan di negara ini.

Kerangka kebijakan yang muncul di Indonesia seputar tata kelola data berkisar pada pemikiran 'kedaulatan data'. Tata kelola data di Indonesia tampaknya masih lebih didominasi pendekatan negara (*state-centered*). Bagi pemerintah dan industri teknologi Indonesia, kolonialisme data tampaknya masih didefinisikan dalam kerangka penggunaan data dari masyarakat di negara-negara berkembang oleh perusahaan-perusahaan teknologi besar asing, yang umumnya berasal dari negara-negara Barat, untuk, memperkaya diri mereka sendiri. Kolonialisme data di sini dipahami sebagai permasalahan geopolitik di mana negara-negara Barat, sekali lagi, berupaya "menjajah" negara-negara Selatan dalam kerangka kolonialisme data. Data diperlakukan sebagai aset yang diproduksi secara nasional dan harus dikontrol oleh pemerintah. Asumsi mendasar dalam kerangka kebijakan pemerintah Indonesia adalah bahwa pemerintah akan secara adil mendistribusikan berbagai manfaat yang diperoleh dari ekstraksi nilai komersial dari data "milik Indonesia" sekaligus melindunginya dari perusahaan dan pemerintah asing.

Secara teoritis memang terdapat ruang bagi pengaturan pemerintah yang dilakukan berdasarkan konsep pemerintah sebagai penjamin kepentingan umum. Dalam konteks ini, terlihat bahwa peran pemerintah Indonesia dalam memperjuangkan prinsip kedaulatan data, dilakukan berdasarkan prinsip 'kedaulatan' yang dipahami sebagai sesuatu yang beroperasi utamanya di level negara. Contohnya adalah ketika upaya pemerintah untuk melakukan lokalisasi data lebih ditekankan pada pendekatan utama yang berakar pada prinsip kedaulatan negara. Artinya, setiap data yang dihasilkan dalam batas wilayah suatu negara adalah aset nasional yang sepenuhnya tunduk pada kewenangan negara. Namun, dalam model kedaulatan data semacam itu, diasumsikan bahwa karena pemerintah secara teori adalah perwakilan dari kehendak rakyat, maka kewenangannya yang luas dalam mengelola data berjalan sesuai dengan pemahaman bahwa individu warga negara memiliki kemampuan untuk memiliki kendali atas data yang mereka miliki. Dalam kerangka kebijakan semacam ini, pemerintah memiliki kewenangan yang besar dalam mengontrol data warga negaranya, namun di saat yang bersamaan belum ada kejelasan sejauh mana masyarakat memiliki hak untuk

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

menentukan bagaimana pemerintah beserta entitas non-pemerintah yang diberikan kuasa sebagai pengelola data-menggunakan data mereka. Dalam kondisi yang demikian, UU Perlindungan Data Pribadi sangat mungkin tidak memiliki kemampuan dalam memberdayakan individu untuk memiliki kebebasan secara ekonomi atau politik dalam memilih bagaimana data mereka digunakan.

Mencermati hal tersebut, kita dapat berargumen bahwa, berdasarkan paradigma tata kelola data yang ada di Indonesia saat ini, pemerintah dan perusahaan dianggap "satu-satunya aktor yang benar-benar memiliki kekuasaan dan kapasitas untuk terlibat dalam proses pengumpulan, penyimpanan, dan analisis data, sementara masyarakat dipersepsikan sebagai pihak yang secara alami mendapatkan keuntungan dari hal-hal tersebut. Yang harus menjadi catatan di sini adalah, pemikiran semacam ini mengingatkan kita pada argumen yang diklaim menjadi dasar 'proyek penyebaran peradaban' kolonialisme barat di masa lalu. Seperti yang dicatat Sinha & Basu (2021), pengewantahan dari kedaulatan data oleh pemerintah suatu negara tidak boleh melemahkan akar kedaulatan tersebut. Dengan kata lain, "…kontrol yang lebih besar dari pemerintah di negara-negara berkembang terhadap ekosistem tata kelola data di masa modern sekarang ini tidak boleh dilakukan dengan mengorbankan otonomi individu atau komunitas...".

Oleh karena itu, sangat dibutuhkan regulasi yang mampu mewadahi dan memberikan jaminan keamanan data pribadi tiap warga negara. UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi belum lama disahkan dan perlu dicermati untuk implementasinya ke depan. Pembangunan kapabilitas warga negara Indonesia terkait keamanan data juga sangat dibutuhkan. Dalam hal ini, negara memiliki tanggung jawab dalam membentuk tata kelola data yang mampu memberikan perlindungan data yang aman juga demokratis bagi warga negara Indonesia. Pendekatan *people centered* dengan mengedepankan konteks *data as social labour* merupakan solusi untuk mengakselerasi pembangunan keamanan siber dan kedaulatan data di Indonesia. Dengan pendekatan ini akan memberikan kebebasan bagi masing-masing warga negara dalam menjaga data-data pribadi mereka. Kesadaran keamanan data dan informasi berpotensi meningkat sehingga berimplikasi pada peningkatan kapabilitas warga negara terkait proteksi data pribadinya.

IV. PENUTUP

Persoalan mendasar dalam kerangka tata kelola data di Indonesia adalah persepsi bahwa data hanya dipandang sebagai sumber daya. Pandangan ini memfasilitasi eksploitasi yang dilakukan oleh perusahaan swasta, di satu sisi, atau mendorong pemerintah untuk memperlakukannya semata-mata sebagai aset nasional. Namun, metafora 'data sebagai sumber daya' mengabaikan karakteristik sosial data. Seperti yang dijelaskan oleh Svensson & Guillen (2020), data, secara prinsipil, tidak pernah 'diberikan' begitu saja. Data sesungguhnya dihasilkan oleh masyarakat dengan tingkat jejaring yang sangat intensif. Kondisi inilah yang memungkinkan data dikumpulkan, dikuantifikasi, dan diproses. Berbagai proses tersebut memberikan bentuk tertentu pada data, yang menunjukkan bahwa "data sangat bersifat kultural dan memiliki kandungan norma dan nilai masyarakat. Dengan kata lain, data tidak sekonyong-konyong muncul secara alami ketika dikumpulkan dan dimanipulasi oleh manusia, bahkan ketika itu dibentuk oleh keputusan, interpretasi, dan filter dari manusia". Dengan demikian, data pribadi (informasi alamiah yang dapat diidentifikasi dari seseorang) maupun data non-

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

pribadi (seperti informasi cuaca atau data kesehatan yang bersifat anonim) sesungguhnya memiliki karakter sosial. Sebelum data menjadi aset perusahaan atau nasional, data pertama-tama dihasilkan oleh manusia, oleh entitas-entitas yang berada dalam dunia sosial.

Aspek lain dari tata kelola data yang harus dipertimbangkan oleh para pembuat kebijakan di Indonesia adalah kenyataan bahwa data menghubungkan manusia satu dengan yang lain. Data dikumpulkan, diproses, dan digunakan secara relasional. Data mengklasifikasikan, mengurutkan, dan mengkategorikan individu dalam kaitannya antara satu sama lain (Viljoen, 2020). Model bisnis dan pemerintahan akan melanggengkan kesenjangan sosial dengan melihat data di dalamnya murni dari segi ekonomi, hanya sebagai sumber daya yang dilucuti dari dimensi sosial atau dimensi yang terkandung di dalamnya. Datafikasi, yaitu produksi data atau bagaimana aspek kehidupan diubah menjadi data, dapat menghasilkan relasi data yang memperkuat dan mencerminkan kesenjangan sosial. Terlebih lagi mengabaikan dimensi sosial dari data juga berarti mengabaikan kemungkinan produksi data yang bermanfaat secara sosial. Pada akhirnya Indonesia diharapkan akan dapat berkontribusi dalam menciptakan kerangka dekolonial yang kuat, dengan meninggalkan metafora konsep 'data sebagai sumber daya' dan membingkai ulang metafora konsep data untuk menekankan aspek sosial dan aspek lainnya yang terkandung dalam data. Pemerintah juga diharapkan dapat membangun otoritas PDP yang independen untuk membangun kepercayaan masyarakat terhadap perlindungan data pribadi dan mendorong akselerasi transformasi digital yang berkesinambungan.

Privasi individu dan keamanan data haruslah menjadi prioritas. Dalam mengatasi permasalahan ini, semakin berkembang peraturan yang mencakup persyaratan yang ketat mengenai perlindungan data pribadi, persetujuan penggunaan data, serta langkah-langkah keamanan siber yang diperlukan melindungi data sensitif. Namun, juga penting untuk menemukan keseimbangan yang tepat antara perlindungan privasi dan data keamanan dengan perlunya kelancaran perdagangan internasional. Terlalu banyak peraturan dapat menghambat aliran data lintas batas Oleh karena itu, tantangan bagi hukum perdagangan internasional adalah mengembangkan kerangka kerja yang seimbang, yang memungkinkan terjadinya perdagangan digital yang efisien sambil memastikan privasi dan keamanan data yang memadai. Kerjasama internasional dalam mengatasi masalah ini sangat penting, karena masalah privasi dan keamanan data sering kali bersifat lintas batas.

DAFTAR PUSTAKA

Arner, D. W., Castellano, G., & Selga, E. (2021). The Transnational Data Governance Problem (University of Hong Kong Faculty of Law Research Paper No. 2021/039). Berkeley Technology Law Journal, Forthcoming. http://dx.doi.org/10.2139/ssrn.3912487

Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. Big Data & Society, 8(1). https://doi.org/10.1177/20539517211017308

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

Basu, A., & Nachiappan, K. (2020). India and the Global Battle For Data Governance (Seminar Paper). India & Digital Worldmaking. https://www.india-seminar.com/2020/731.htm

Basu, A., Hickok, E., & Chawla, A. S. (2019, March 19). The Localisation Gambit. Centre for Internet and Society. https://cis-india.org/internet-governance/blog/the-localisation-gambit-unpacking-policy-moves-for-the-sovereign-control-of-data-in-india

Callaghan, C. W. (2019). *"*Transcending The Threshold Limitation: A Fifth Industrial Revolution?*". Management Research Review , 43 (4), 447-461.*

Chen, H., Chiang, R.H., & Storey, V.C. (2012). "Business Intelligence and Analytics: From Big Data To Big Impact". *MIS quarterly , 1165-1188*

Ciuriak, D. (2022). Unfree Flow with No Trust: The Implications of Geoeconomics and Geopolitics for Data and Digital Trade. Centre for International Governance Innovation. http://dx.doi. org/10.2139/ssrn.3963074

Costa, C. M., Martinez-Galán, E., & Leandro, F. J. (2022). *"*Does Fifth Industrial Revolution Benefit or Trouble Global Civil Society?" Dalam *Contestations in Global Civil Society (pp. 45-62). Emerald Publishing Limited.*

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. Television & New Media, 20(4), 336–349.

Cohen, Julie E. (2019); *Between Truth and Power: The Legal Constructions of Informational Capitalism* ; New York, Oxford University Press.

George, AS, & George, A.H. (2020). Industrial Revolution 5.0: The Transformation of The Modern Manufacturing Process to Enable Man And Machine to Work Hand in Hand*. Journal of Seybold Report, ISSN NO , 1533 , 9211*

Kovacs, A., & Ranganathan, N. (2019). Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India (Working Paper 03). Data Governance Network. https:// datagovernance.org/files/research/IDP_-_Data_sovereignty_-_Paper_3.pdf

Lesmana, CSA Teddy; Elis, Eva; dan Hamimah, Siti, (2022) "Urgensi Undang-Undang Perlindungan Data Pribadi dalam Menjamin Keamanan Data Pribadi sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia* 3, no. 2 (Juni 21, 2022): 2, https://rechten.nusaputra.ac.id/article/view/78.

Mehmood, T. (2021). "Do Information Technology Competencies and Fleet Management Practices Lead to Effective Service Delivery? Empirical Evidence from The E-Commerce Industry*". International Journal of Technology, Innovation and Management (IJTIM) ,* 1 (2), 14-41.

Obar, Jonathan A. & Oeldorf-Hirsch, Anne, (2018); "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services", *Information, Communication, and Society*, 128.

Puschmann, C., & Burgess, J. (2014). Big data, big questions: Metaphors of big data. International Journal of Communication, (8), 1690–1709. https://ijoc.org/index.php/ijoc/ article/view/2169/1162

Ravlindo, E., & Gunadi, A. (2022). Perlindungan Hukum Terhadap Data Kesehatan Melalui Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi. *Jurnal Hukum Adigama,* 4(2), 4748–4769

p-ISSN : 3032-6699
E-ISSN : 3032-7083
Volume 1, Desember 2023

Regan, Priscilla M. (1995); *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, University of North Carolina Press.

Richards, Neil M. and Hartzog, Woodrow, (2019); The Pathologies of Digital Consent (April 11, 2019). 96 *Washington University Law Review* 1461.

Sinha, A., & Basu, A., (2021, August 13). Why Metaphors for Data Matter. Bot Populi. https://botpopuli.net/why-metaphors-for-data-matter/

Sudibyo (2019), Agus; *Jagat Digital, Pembebasan dan Penguasaan* (Jakarta: Kepustakaan Populer Gramedia, 2019).

The Economist. (2017, May 6). Data is giving rise to a new economy. https://www.economist.com/ briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

Viljoen, S. (2021). A relational theory of data governance. Yale Law Journal, (131), 573–654. https://www.yalelawjournal.org/pdf/131.2_Viljoen_1n12myx5.pdf

Zuboff, Shoshana, and Karin Schwandt. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London, England: Profile Books