DARURAT DATA NASIONAL

KRISIS KEDAULATAN DATA RAKYAT INDONESIA

Kajian ini menganalisis fenomena kebocoran data di Indonesia sebagai permasalahan struktural yang memiliki implikasi luas terhadap kedaulatan data nasional. Dalam beberapa tahun terakhir, Indonesia mengalami peningkatan signifikan dalam insiden kebocoran data, dengan jumlah yang mencapai puluhan juta data setiap tahun serta dominasi kejadian pada sektor publik yang seharusnya menjadi garda terdepan dalam perlindungan data. Kondisi ini menunjukkan bahwa kebocoran data tidak lagi bersifat insidental, melainkan telah berkembang menjadi fenomena sistemik yang mencerminkan adanya kelemahan dalam tata kelola data nasional.

Kajian ini menggunakan pendekatan kualitatif deskriptif-analitis dengan mengintegrasikan data empiris, analisis kebijakan, serta kerangka teori yang meliputi teori tata kelola data (data governance), kapasitas negara (state capacity), dan kedaulatan digital (data sovereignty). Hasil analisis menunjukkan bahwa tingginya frekuensi kebocoran data, lemahnya mekanisme pengawasan, serta belum optimalnya penegakan regulasi menciptakan kesenjangan antara norma hukum dan praktik di lapangan (governance gap). Selain itu, meningkatnya arus data lintas negara dalam ekonomi digital global turut memperbesar risiko erosi kontrol negara terhadap data warganya.

Lebih lanjut, kajian ini menyoroti rendahnya tingkat kesadaran publik terhadap risiko kebocoran data sebagai faktor yang memperparah kerentanan masyarakat. Kondisi ini menciptakan ketimpangan antara tingkat ancaman yang tinggi dan kapasitas perlindungan individu yang masih terbatas (awareness gap). Dalam konteks tersebut, masyarakat tidak hanya menjadi objek dari sistem pengelolaan data, tetapi juga pihak yang paling terdampak dari kelemahan sistem tersebut.

Kajian ini menyimpulkan bahwa kebocoran data di Indonesia telah berkembang menjadi krisis multidimensi yang melibatkan aspek teknis, kelembagaan, ekonomi, dan sosial, serta berpotensi melemahkan kedaulatan data nasional. Oleh karena itu, diperlukan langkah strategis yang komprehensif, meliputi penguatan kelembagaan pengawas, peningkatan standar keamanan data, pengaturan transfer data lintas negara, serta peningkatan literasi dan kesadaran publik. Dengan demikian, perlindungan data pribadi tidak hanya menjadi isu kebijakan, tetapi juga bagian dari upaya kolektif dalam menjaga kedaulatan negara di era digital.

PENDAHULUAN

Perkembangan teknologi digital dalam dua dekade terakhir telah mengubah secara fundamental cara masyarakat berinteraksi, bekerja, dan mengakses layanan publik. Data pribadi kini menjadi elemen yang tidak terpisahkan dari kehidupan sehari-hari, di mana hampir seluruh aktivitas digital—mulai dari penggunaan media sosial, transaksi keuangan, layanan kesehatan, hingga administrasi pemerintahan—melibatkan pengumpulan dan pemrosesan data dalam skala besar. Dalam konteks ini, data tidak lagi sekadar informasi pasif, melainkan telah berkembang menjadi aset strategis yang memiliki nilai ekonomi, sosial, dan politik.

Sejalan dengan hal tersebut, literatur ekonomi digital menempatkan data sebagai sumber daya utama dalam ekonomi modern. Nick Srnicek (2017) https://politybooks.com/bookdetail/?isbn=9781509504862 dalam Platform Capitalism menegaskan bahwa data merupakan “bahan baku” utama dalam proses akumulasi nilai oleh platform digital.

Shoshana Zuboff (2019) melalui konsep surveillance capitalism menjelaskan bahwa data pribadi tidak hanya dikumpulkan, tetapi juga dimonetisasi dan digunakan untuk memprediksi serta memengaruhi perilaku individu.

Namun demikian, peningkatan ketergantungan terhadap sistem digital tidak diiringi dengan pemahaman dan kesiapan yang memadai dalam aspek perlindungan data. Di Indonesia, berbagai insiden kebocoran data yang terjadi secara berulang menunjukkan adanya kerentanan sistemik dalam pengelolaan data pribadi. Kebocoran data tidak hanya terjadi pada sektor privat, tetapi juga melibatkan institusi publik yang seharusnya memiliki tanggung jawab utama dalam melindungi data warga negara.

Dalam perspektif keamanan siber, fenomena ini dapat dipahami sebagai bentuk systemic vulnerability, yaitu kondisi di mana kelemahan tidak lagi bersifat individual atau teknis semata, melainkan melekat pada struktur sistem secara keseluruhan. Ross Anderson (2001) https://www.cl.cam.ac.uk/~rja14/book.html Dalam Security Engineering menekankan bahwa kegagalan dalam perlindungan data sering kali disebabkan oleh lemahnya insentif kelembagaan dan kurangnya akuntabilitas.

Lebih lanjut, dari sudut pandang tata kelola, masalah kebocoran data mencerminkan adanya kesenjangan antara regulasi dan implementasi. Christopher Kuner et al. (2020) https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491 dalam The EU General Data Protection Regulation (GDPR): A Commentary menegaskan bahwa efektivitas perlindungan data sangat bergantung pada mekanisme pengawasan dan penegakan hukum yang kuat.

Di sisi lain, kebocoran data juga memiliki implikasi langsung terhadap hubungan antara negara dan warga negara. Francis Fukuyama (2013) dalam What Is Governance?

menjelaskan bahwa kapasitas negara ditentukan oleh kemampuannya dalam menjalankan fungsi perlindungan terhadap masyarakat.

Dalam konteks yang lebih luas, fenomena kebocoran data juga berkaitan dengan isu kedaulatan. Luciano Floridi (2020) dalam kajian mengenai digital sovereignty menyatakan bahwa kemampuan negara dalam mengendalikan dan melindungi data warganya merupakan bagian penting dari kedaulatan modern.

Selain aspek struktural dan kelembagaan, faktor lain yang tidak kalah penting adalah rendahnya tingkat kesadaran publik terhadap risiko kebocoran data. Dalam laporan European Union Agency for Cybersecurity (ENISA) kondisi ini disebut sebagai *awareness gap*, yaitu kesenjangan antara tingkat ancaman dan pemahaman masyarakat terhadap risiko digital.

Dalam konteks tersebut, kebocoran data tidak dapat lagi dipandang sebagai persoalan teknis semata, melainkan sebagai persoalan multidimensi yang mencakup aspek teknologi, hukum, ekonomi, dan sosial. Oleh karena itu, kajian ini tidak hanya bertujuan untuk menganalisis fenomena kebocoran data di Indonesia, tetapi juga untuk memberikan kontribusi dalam meningkatkan pemahaman publik mengenai pentingnya perlindungan data pribadi. Lebih jauh, kajian ini berupaya menempatkan isu kebocoran data dalam kerangka kedaulatan nasional, sehingga dapat dipahami sebagai bagian dari tantangan strategis negara di era digital.

KONDISI EMPIRIS

Kebocoran data di Indonesia dalam beberapa tahun terakhir menunjukkan tren peningkatan yang signifikan, baik dari sisi jumlah insiden maupun skala data yang terekspos. Fenomena ini menandakan bahwa Indonesia menghadapi tantangan serius dalam aspek keamanan siber dan perlindungan data pribadi.

Skala Kebocoran Data

Sejumlah laporan menunjukkan bahwa kebocoran data di Indonesia telah mencapai tingkat yang mengkhawatirkan:

- Pada tahun 2024, diperkirakan lebih dari 56 juta data terekspos dari berbagai sektor, termasuk pemerintah dan swasta.
- Secara kumulatif, berbagai studi menyebutkan bahwa lebih dari 150 juta data penduduk Indonesia telah bocor dalam periode 2004–2024.
- Indonesia juga termasuk dalam kelompok negara dengan jumlah insiden kebocoran data yang tinggi secara global.

https://www.liputan6.com/tekno/read/6180865

https://banggasemarang.id/2025/10/05/alarm-keras-untuk-indonesia-di-era-digital/

Skala ini menunjukkan bahwa kebocoran data di Indonesia telah melampaui kategori insiden biasa dan masuk dalam kategori ***high exposure risk***, di mana data dalam jumlah besar terekspos secara berulang.

Pola Serangan Siber

Selain jumlah data yang bocor, pola serangan siber juga menunjukkan bahwa data merupakan target utama:

- Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sekitar 62% insiden siber di Indonesia berkaitan dengan pencurian data.
- Pada awal tahun 2025, tercatat 139 kasus serangan digital hanya dalam satu kuartal, menunjukkan peningkatan signifikan dibanding tahun sebelumnya.

https://www.neraca.co.id/article/222694

https://data.goodstats.id/statistic/serangan-digital-di-indonesia-tembus-139-kasus-pada-awal-2025-ZPFZI

Hal ini menunjukkan bahwa:

Data bukan lagi objek pasif, tetapi menjadi target utama dalam ekosistem serangan siber modern. Dalam perspektif akademik, kondisi ini menunjukkan pergeseran dari system disruption ke data ***extraction attack***.

Dominasi Sektor Publik dalam Kebocoran Data

Salah satu temuan penting adalah tingginya keterlibatan sektor publik dalam kebocoran data:

- Sekitar 58,34% data yang beredar di dark web berasal dari sektor pemerintah
- Studi lain menunjukkan bahwa sekitar 63% kebocoran data terjadi di sektor pemerintah dan perbankan

https://www.liputan6.com/tekno/read/6180865

https://www.cypriva.id/articles/kebocoran-data-pribadi-di-indonesia

Temuan ini mengindikasikan bahwa:

institusi yang seharusnya menjadi pelindung data justru menjadi salah satu titik paling rentan dalam sistem. Dalam perspektif state capacity, kondisi ini mencerminkan keterbatasan negara dalam menjalankan fungsi perlindungan digital.

Dampak Empiris Kebocoran Data

Kebocoran data di Indonesia tidak hanya berdampak pada privasi individu, tetapi juga pada aspek ekonomi dan sosial:

- Lebih dari 21,7 juta akun email mengalami pembajakan pada 2024
- Kebocoran data kesehatan (BPJS) yang melibatkan sekitar 279 juta data berpotensi memicu peningkatan klaim fiktif hingga 300%
- Kerugian ekonomi akibat serangan siber diperkirakan mencapai jutaan dolar AS setiap tahun

https://banggasemarang.id/2025/10/05/alarm-keras-untuk-indonesia-di-era-digital/

https://www.cypriva.id/articles/kebocoran-data-pribadi-di-indonesia

Dampak ini menunjukkan bahwa kebocoran data telah berkembang menjadi:

multi-sectoral risk, yang memengaruhi stabilitas ekonomi, kepercayaan publik, dan keamanan sosial.

Karakteristik Umum Fenomena Kebocoran Data di Indonesia

Berdasarkan data empiris di atas, terdapat beberapa karakteristik utama:

1. **Skala besar** → melibatkan jutaan hingga ratusan juta data
2. **Frekuensi tinggi** → terjadi berulang setiap tahun
3. **Target utama adalah data pribadi**
4. **Dominasi sektor publik sebagai sumber kebocoran**
5. **Dampak luas lintas sektor**

Kondisi ini menunjukkan bahwa kebocoran data di Indonesia telah berkembang menjadi fenomena:

systemic data breach, yaitu kebocoran data yang terjadi secara berulang akibat kelemahan struktural dalam sistem, bukan sekadar kesalahan teknis individual.

DIMENSI KESADARAN PUBLIK

Meskipun kebocoran data di Indonesia terjadi dalam skala besar dan menunjukkan tren peningkatan yang signifikan, tingkat kesadaran masyarakat terhadap risiko keamanan data masih relatif rendah. Kondisi ini menciptakan fenomena yang dalam literatur keamanan siber dikenal sebagai *awareness gap*, yaitu kesenjangan antara tingginya tingkat ancaman dan rendahnya tingkat pemahaman masyarakat terhadap risiko tersebut (ENISA, 2018).

Dalam konteks Indonesia, *awareness gap* ini menjadi salah satu faktor yang memperparah kerentanan masyarakat dalam ekosistem digital. Hal ini karena masyarakat tidak hanya menjadi objek dari sistem pengumpulan data, tetapi juga pihak yang paling terdampak ketika terjadi kebocoran data, tanpa memiliki kapasitas perlindungan yang memadai.

Konsep Awareness Gap dalam Keamanan Siber

Menurut European Union Agency for Cybersecurity (ENISA), awareness gap terjadi ketika pengguna teknologi tidak memiliki pemahaman yang sebanding dengan tingkat risiko yang dihadapi dalam penggunaan sistem digital.

Sumber: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines

Selain itu, dalam kajian literasi digital, van Deursen dan van Dijk (2014) menjelaskan bahwa keterbatasan kemampuan pengguna dalam memahami risiko teknologi menyebabkan meningkatnya kerentanan terhadap ancaman digital.

Sumber: https://www.sciencedirect.com/science/article/pii/S0747563213001659

Kondisi ini menunjukkan bahwa keamanan data tidak hanya bergantung pada sistem, tetapi juga pada tingkat literasi pengguna.

Faktor Penyebab Rendahnya Kesadaran Publik

1. Rendahnya Literasi Digital

Literasi digital di Indonesia masih menghadapi tantangan, khususnya dalam aspek keamanan data. Berdasarkan laporan Kementerian Komunikasi dan Informatika (Kominfo), indeks literasi digital Indonesia masih berada pada kategori sedang dan belum merata.

Sumber: https://literasidigital.id

Masyarakat cenderung memahami penggunaan teknologi, tetapi belum memahami risiko di baliknya (functional use without security awareness).

2. Minimnya Transparansi Informasi Kebocoran Data

Banyak kasus kebocoran data tidak disertai dengan komunikasi publik yang memadai. Hal ini menyebabkan masyarakat tidak mengetahui apakah datanya terdampak atau tidak.

Dalam teori risk communication, transparansi merupakan elemen penting dalam membangun kesadaran dan respons publik (Covello, 2003).

Sumber: https://www.ncbi.nlm.nih.gov/books/NBK221472/

Kurangnya transparansi menciptakan kondisi di mana risiko tidak terlihat (invisible risk), sehingga tidak memicu respons publik.

3. Normalisasi Kebocoran Data

Frekuensi kebocoran data yang tinggi tanpa konsekuensi yang jelas menyebabkan masyarakat mulai menganggap kebocoran sebagai hal yang biasa.Dalam perspektif sosiologi risiko (Beck, 1992), kondisi ini disebut sebagai risk normalization, yaitu proses di mana masyarakat menjadi terbiasa dengan risiko yang seharusnya dianggap serius.

Sumber: https://uk.sagepub.com/en-gb/eur/risk-society/book203184

Normalisasi ini berbahaya karena menurunkan sensitivitas masyarakat terhadap ancaman.

Dampak Awareness Gap terhadap Masyarakat

Akibat dari rendahnya kesadaran publik, masyarakat sering kali berada dalam posisi yang rentan, antara lain:

- Tidak mengetahui bahwa data pribadinya telah bocor
- Tidak memahami potensi penyalahgunaan data (penipuan, phishing, dll)

Tidak memiliki langkah mitigasi, seperti:

- mengganti kata sandi
- mengaktifkan autentikasi dua faktor
- memantau aktivitas akun

Dalam konteks ini, masyarakat tidak hanya menjadi korban pasif, tetapi juga bagian dari sistem yang rentan terhadap eksploitasi.

Kondisi ini mencerminkan adanya: ***information asymmetry***, yaitu ketimpangan informasi antara pengelola data dan pemilik data (Stiglitz, 2002)

Implikasi terhadap Kedaulatan Data

Rendahnya kesadaran publik tidak hanya berdampak pada individu, tetapi juga pada skala nasional. Dalam konteks kedaulatan data, masyarakat yang tidak memiliki kesadaran akan risiko data akan sulit berperan dalam mendorong akuntabilitas sistem.

Dengan demikian, awareness gap tidak hanya menjadi persoalan edukasi, tetapi juga menjadi faktor yang berkontribusi terhadap melemahnya kedaulatan data nasional.

POSISI MASYARAKAT DALAM EKOSISTEM DATA

Dalam ekosistem digital kontemporer, masyarakat menempati posisi yang paradoksal. Di satu sisi, individu diwajibkan untuk menyerahkan data pribadi sebagai prasyarat untuk mengakses berbagai layanan, baik yang disediakan oleh negara maupun sektor privat. Proses ini mencakup berbagai aktivitas, mulai dari pendaftaran layanan publik, penggunaan aplikasi digital, hingga transaksi ekonomi berbasis platform. Namun di sisi lain, masyarakat tidak memiliki kontrol penuh terhadap bagaimana data tersebut disimpan, diproses, dibagikan, atau bahkan dilindungi.

Kondisi ini menciptakan ketimpangan struktural antara kewajiban individu dalam menyediakan data dan kapasitas sistem dalam memberikan perlindungan yang memadai. Dalam literatur ekonomi informasi, fenomena ini dikenal sebagai data asymmetry atau information asymmetry, yaitu situasi di mana terdapat ketidakseimbangan informasi dan kekuasaan antara pihak yang mengelola data dan pihak yang menjadi sumber data (Stiglitz, 2002).

Sumber: https://www.nobelprize.org/prizes/economic-sciences/2001/stiglitz/facts/

Data sebagai Syarat Partisipasi Digital

Dalam sistem digital modern, data pribadi menjadi “tiket masuk” untuk berpartisipasi dalam kehidupan sosial dan ekonomi. Tanpa memberikan data, individu sering kali tidak dapat mengakses layanan dasar seperti:

- administrasi kependudukan
- layanan kesehatan
- sistem keuangan digital
- platform komunikasi

Zuboff (2019) menyebut kondisi ini sebagai bagian dari surveillance capitalism, di mana individu tidak memiliki pilihan nyata selain berpartisipasi dalam sistem yang mengekstraksi data mereka.

Partisipasi digital bersifat ***mandatory***, bukan pilihan bebas, sehingga individu berada dalam posisi yang lemah secara struktural.

Keterbatasan Kontrol Individu terhadap Data

Meskipun individu menjadi sumber utama data, kontrol terhadap data tersebut sebagian besar berada di tangan:

- penyelenggara sistem elektronik
- platform digital
- institusi pemerintah

Dalam praktiknya, individu memiliki keterbatasan dalam:

- mengetahui bagaimana data digunakan
- mengontrol distribusi data
- menghapus atau menarik data
- menuntut pertanggungjawaban secara efektif

Kuner et al. (2020) menekankan bahwa tanpa mekanisme kontrol yang jelas, hak atas data pribadi cenderung bersifat normatif, tetapi tidak operasional.

Sumber: https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491

Hak individu terhadap data sering kali tidak diimbangi dengan kapasitas aktual untuk mengontrol data tersebut (control illusion).

Data Asymmetry sebagai Ketimpangan Struktural

Konsep data asymmetry menjelaskan bahwa terdapat ketimpangan antara:

- pihak yang mengumpulkan dan memproses data (negara dan korporasi)
- dan pihak yang menjadi sumber data (masyarakat)

Dalam konteks ini:

- Pengelola data memiliki akses, kontrol, dan kapasitas analisis
- Masyarakat hanya memiliki peran sebagai penyedia data

Stiglitz (2002) menunjukkan bahwa ketimpangan informasi ini dapat menciptakan ketidakseimbangan kekuasaan dalam sistem ekonomi dan sosial.

Dalam ekosistem digital, data asymmetry berkembang menjadi: asymmetry of power, di mana kontrol atas data berarti kontrol atas informasi, keputusan, dan bahkan perilaku

Implikasi Sosial dan Politik

Ketimpangan dalam pengelolaan data tidak hanya berdampak pada individu, tetapi juga memiliki implikasi sosial dan politik yang lebih luas, antara lain:

- **Kerentanan individu terhadap eksploitasi data**
  Data dapat digunakan untuk penipuan, profiling, dan manipulasi
- **Menurunnya posisi tawar masyarakat**
  Individu tidak memiliki kendali atas aset digitalnya sendiri
- **Melemahnya kepercayaan terhadap sistem digital**
  Ketika data tidak aman, legitimasi sistem ikut terpengaruh
- **Potensi dominasi aktor besar (negara/korporasi)**
  Data menjadi alat kontrol dalam ekosistem digital

Dalam perspektif digital political economy, kondisi ini mencerminkan konsentrasi kekuasaan pada pihak yang menguasai data (Srnicek, 2017).

Sumber: https://politybooks.com/bookdetail/?isbn=9781509504862

Implikasi terhadap Kedaulatan Data

Ketimpangan posisi masyarakat dalam ekosistem data juga berdampak pada kedaulatan data nasional. Negara yang tidak mampu memastikan keseimbangan antara:

- pengumpulan data
- perlindungan data
- dan kontrol individu

akan menghadapi risiko:

melemahnya kedaulatan data secara internal.

Floridi (2020) menekankan bahwa kedaulatan digital tidak hanya bergantung pada kontrol negara, tetapi juga pada perlindungan terhadap individu sebagai pemilik data.

Sumber: https://link.springer.com/article/10.1007/s13347-020-00402-8

Berdasarkan analisis di atas, dapat disimpulkan bahwa:

- Masyarakat berada dalam posisi yang tidak seimbang dalam ekosistem data
- Data menjadi kewajiban untuk partisipasi, tetapi tidak diiringi kontrol
- Terjadi data asymmetry yang menciptakan ketimpangan kekuasaan
- Kondisi ini memperbesar kerentanan individu dan melemahkan sistem secara keseluruhan

Dalam ekosistem digital saat ini, masyarakat tidak hanya menjadi pengguna sistem, tetapi juga menjadi sumber data tanpa kontrol yang memadai, yang pada akhirnya menciptakan ketimpangan struktural dalam pengelolaan data.

KETIDAKSIAPAN SISTEM NASIONAL MENGHADAPI LIBERALISASI DATA GLOBAL

Implikasi Perjanjian Art Terhadap Kedaulatan Data Nasional

Perjanjian ART mendorong liberalisasi arus data lintas negara melalui kewajiban untuk memfasilitasi transfer data secara elektronik. Namun, kondisi empiris di Indonesia menunjukkan bahwa sistem keamanan data nasional masih berada dalam kondisi rentan, ditandai dengan tingginya frekuensi kebocoran data dan lemahnya tata kelola perlindungan data .

Permasalahan utama terletak pada ketidaksesuaian antara arah kebijakan liberalisasi data dengan kapasitas sistem domestik yang belum siap. Dalam kondisi di mana kebocoran data telah bersifat sistemik, pembukaan arus data lintas negara justru berpotensi memperbesar risiko kebocoran dan penyalahgunaan data.

Ketentuan dalam perjanjian yang mengharuskan kelancaran arus data lintas negara berimplikasi pada berkurangnya ruang kontrol negara terhadap data yang berada dalam yurisdiksinya .

Permasalahan ini berkaitan langsung dengan kedaulatan data, di mana negara seharusnya memiliki kewenangan penuh untuk:

- menentukan lokasi penyimpanan data
- mengatur distribusi data
- membatasi akses terhadap data strategis

Dengan adanya kewajiban internasional tersebut, negara menghadapi keterbatasan dalam menjalankan fungsi pengendalian, yang pada akhirnya berpotensi melemahkan kedaulatan digital nasional.

Indonesia telah memiliki kerangka hukum melalui Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mengatur bahwa transfer data ke luar negeri harus memenuhi persyaratan tertentu. Namun, perjanjian ART mengarah pada kewajiban untuk membuka arus data lintas negara.

Permasalahan muncul ketika ketentuan internasional berpotensi membatasi penerapan regulasi nasional. Dalam kondisi tersebut, terdapat risiko bahwa:

- regulasi nasional harus disesuaikan
- atau implementasinya menjadi tidak optimal

Hal ini menciptakan ketegangan antara kepentingan perlindungan data domestik dan kewajiban dalam perjanjian internasional.

Dalam ekosistem digital global, penguasaan teknologi dan infrastruktur data didominasi oleh perusahaan besar yang sebagian besar berasal dari negara maju. Sementara itu, Indonesia berada pada posisi sebagai penyedia data dalam skala besar.

Permasalahan yang muncul adalah terjadinya ketimpangan kekuasaan (asymmetry of power), di mana:

- aktor global memiliki kontrol terhadap data dan teknologi
- negara dan masyarakat memiliki keterbatasan kontrol

Kajian menunjukkan bahwa kondisi ini mencerminkan adanya data asymmetry, yaitu ketidakseimbangan antara pengelola data dan pemilik data . Perjanjian ART berpotensi memperkuat ketimpangan ini.

Risiko terhadap Keamanan Nasional Berbasis Data

Data dalam era digital memiliki nilai strategis yang tidak hanya terbatas pada aspek ekonomi, tetapi juga mencakup aspek keamanan nasional .

Dengan terbukanya arus data lintas negara, terdapat risiko bahwa data strategis:

- berada di luar yurisdiksi Indonesia
- tunduk pada hukum negara lain
- dapat diakses oleh pihak asing

Permasalahan ini menunjukkan bahwa liberalisasi data tidak hanya berdampak pada sektor ekonomi, tetapi juga berpotensi mengancam keamanan nasional secara lebih luas.

Melemahnya Posisi Individu sebagai Subjek Data

Kajian menunjukkan bahwa masyarakat Indonesia berada dalam posisi yang lemah dalam ekosistem data, dengan keterbatasan kontrol terhadap data pribadi mereka .

Permasalahan menjadi semakin kompleks dengan adanya liberalisasi arus data, yang:

- memperluas distribusi data tanpa kontrol individu
- meningkatkan potensi eksploitasi data
- memperburuk ketimpangan antara pengelola dan pemilik data

Dalam kondisi ini, individu tidak hanya menjadi objek sistem data, tetapi juga pihak yang paling terdampak dari kelemahan sistem tersebut.

Penyempitan Ruang Kebijakan Negara (Policy Space)

Perjanjian ART membatasi kemampuan negara dalam mengatur kebijakan terkait data, termasuk dalam hal:

- pembatasan transfer data
- penerapan data localization
- regulasi terhadap platform digital

Padahal, kajian menekankan pentingnya pengaturan ketat terhadap transfer data lintas negara untuk menjaga kedaulatan data .

Permasalahan ini menunjukkan bahwa ruang kebijakan negara menjadi semakin terbatas, sehingga menyulitkan pemerintah dalam merespons dinamika dan risiko di masa depan.

Pelebaran Kesenjangan Tata Kelola (Governance Gap)

Kajian menunjukkan adanya kesenjangan antara norma hukum dan praktik di lapangan dalam pengelolaan data di Indonesia .

Permasalahan menjadi semakin kompleks ketika perjanjian ART menambah kewajiban baru tanpa diiringi peningkatan kapasitas kelembagaan. Dalam kondisi ini:

- pengawasan data menjadi lebih sulit
- penegakan hukum menjadi lebih lemah
- akuntabilitas sistem semakin berkurang

Dengan demikian, perjanjian ini berpotensi memperlebar governance gap yang sudah ada.

PENUTUP

Kebocoran data di Indonesia tidak hanya mencerminkan kelemahan sistem teknis, tetapi juga menunjukkan adanya persoalan struktural dalam tata kelola data nasional. Fenomena ini menegaskan bahwa perlindungan data pribadi belum sepenuhnya menjadi prioritas strategis dalam pembangunan digital Indonesia.

Dalam era digital, setiap individu merupakan bagian dari ekosistem data yang saling terhubung. Namun, posisi masyarakat yang rentan—ditandai dengan kewajiban memberikan data tanpa diimbangi kontrol yang memadai—menunjukkan adanya ketimpangan yang perlu segera diperbaiki. Oleh karena itu, perlindungan data pribadi tidak dapat semata-mata diserahkan kepada mekanisme sistem dan regulasi, tetapi juga memerlukan peningkatan kesadaran publik sebagai fondasi utama.

Lebih lanjut, kajian ini menegaskan bahwa krisis kebocoran data yang terjadi saat ini telah mencapai tingkat yang memerlukan respons serius dan terstruktur. Dalam konteks tersebut, diperlukan dorongan kolektif untuk memperkuat tata kelola data nasional melalui sejumlah tuntutan kebijakan yang bersifat mendasar, antara lain:

1. **Penguatan kelembagaan pengawas data pribadi**
   Negara perlu memastikan keberadaan otoritas pengawas yang independen, transparan, dan memiliki kewenangan penegakan hukum yang efektif.
2. **Transparansi penuh terhadap setiap insiden kebocoran data**
   Setiap kebocoran data harus diinformasikan secara terbuka kepada publik sebagai bentuk akuntabilitas dan perlindungan terhadap masyarakat.
3. **Standarisasi keamanan data nasional yang wajib dan terukur**
   Seluruh penyelenggara sistem, baik publik maupun privat, harus memenuhi standar minimum keamanan data yang diaudit secara berkala.
4. **Penguatan hak masyarakat sebagai subjek data**
   Masyarakat harus memiliki akses, kontrol, dan mekanisme perlindungan yang nyata terhadap data pribadinya, bukan sekadar hak normatif dalam regulasi.
5. **Pengaturan ketat terhadap transfer data lintas negara**
   Negara perlu memastikan bahwa setiap aliran data ke luar yurisdiksi tetap berada dalam kontrol hukum nasional dan tidak merugikan kepentingan rakyat.
6. **Peningkatan literasi dan kesadaran publik secara masif**
   Edukasi mengenai keamanan data harus menjadi bagian dari agenda nasional agar masyarakat mampu memahami risiko dan melindungi dirinya dalam ekosistem digital.

Dengan demikian, penguatan kedaulatan data tidak hanya bergantung pada reformasi kebijakan dan sistem, tetapi juga pada meningkatnya kesadaran kolektif masyarakat. Ketika masyarakat memahami posisi, risiko, dan haknya dalam ekosistem digital, maka akan terbentuk dorongan yang lebih kuat untuk menciptakan tata kelola data yang aman, adil, dan akuntabel.

Pada akhirnya, perlindungan data pribadi bukan hanya persoalan teknologi atau regulasi, tetapi merupakan bagian dari upaya menjaga kedaulatan negara dan martabat warga negara di era digital.