

## TANTANGAN ETIKA DAN KEAMANAN DATA DALAM INTEGRASI BIG DATA SEKTOR PUBLIK

Hikmah Widiawati<sup>1\*</sup>, Keke Dana Fiscarina<sup>2</sup>, Erislan<sup>3</sup>

<sup>1,2,3</sup> Universitas Sahid Jakarta

<sup>1</sup> [hikmah.widiawati@usahid.ac.id](mailto:hikmah.widiawati@usahid.ac.id)

\* Corresponding Author

Received: 03-07- 2026

Revised: 10-07-2026

Approved: 22-07-2026

### ABSTRACT

*The integration of information systems and big data in the public sector creates opportunities to improve government service quality, operational efficiency, and data-driven decision-making. However, rapid technological adoption generates increasingly complex challenges related to data ethics and citizen information security, particularly amid the growth of generative artificial intelligence and hybrid cloud computing. This study aims to identify, analyze, and map the ethical and data security challenges faced by public institutions in adopting integrated big data ecosystems. The study employed a systematic literature review (SLR) with a qualitative descriptive approach, examining 58 relevant scientific publications published between 2020 and 2025. The literature was analyzed using thematic synthesis through systematic coding, categorization, and grouping of recurring findings into major themes. The findings identify five major challenges: (1) privacy violations arising from mass data collection and citizen profiling without explicit consent; (2) increased cybersecurity risks within integrated information infrastructures; (3) algorithmic bias and unfairness in AI-based automated decision-making; (4) gaps in the implementation of personal data protection regulations at the regional level; and (5) weak cross-institutional data governance. Unlike previous reviews that tend to examine data ethics, cybersecurity, or digital transformation separately, this study develops an integrated framework linking ethical challenges, security risks, regulatory gaps, and governance weaknesses. This contribution provides a comprehensive foundation for future research and policy development. The study recommends strengthening data governance, implementing Privacy by Design and Security by Default, adopting AI ethics frameworks, and developing human resource capacity.*

**Keywords:** Big Data; Data Governance; Data Ethics; Cybersecurity; Public Sector.

### INTRODUCTION

#### Pendahuluan

Transformasi digital pemerintahan yang berlangsung sangat pesat dalam lima tahun terakhir telah menempatkan *big data* dan *artificial intelligence* (AI) sebagai fondasi utama modernisasi tata kelola serta pelayanan publik. Pemanfaatan teknologi tersebut memungkinkan pemerintah mengintegrasikan berbagai sumber data, menghasilkan analisis secara lebih cepat, serta mendukung proses pengambilan keputusan yang semakin akurat, adaptif, dan berbasis bukti. Integrasi sistem informasi juga mendorong peningkatan efisiensi administrasi, transparansi, akuntabilitas, serta kualitas layanan yang diterima masyarakat. Laporan OECD menunjukkan bahwa lebih dari 70% negara anggotanya telah memiliki strategi nasional AI yang secara eksplisit diarahkan untuk mendukung penyelenggaraan pemerintahan [1]. World Bank juga menegaskan bahwa tingkat kematangan GovTech menjadi indikator penting dalam mengukur kesiapan pemerintah memanfaatkan teknologi digital, tata kelola data, dan layanan publik berbasis elektronik secara berkelanjutan [2]. Rekomendasi G20 India Presidency

menekankan pentingnya penerapan AI yang bertanggung jawab (*Responsible AI*) melalui prinsip transparansi, akuntabilitas, keadilan, keamanan, dan perlindungan hak asasi manusia dalam sektor publik [3]. ASEAN turut mendorong negara-negara anggotanya mengembangkan tata kelola AI yang berlandaskan etika, pengelolaan risiko, serta perlindungan data pribadi sebagai fondasi transformasi digital kawasan [4]. Berbagai inisiatif tersebut menunjukkan bahwa pemanfaatan AI dan *big data* bukan lagi sekadar inovasi teknologi, melainkan telah menjadi bagian dari strategi pembangunan pemerintahan modern di tingkat global. Kondisi tersebut memperlihatkan semakin kuatnya pergeseran paradigma menuju pemerintahan berbasis data (*data-driven government*) yang menempatkan data sebagai aset strategis dalam perumusan kebijakan publik.

Indonesia turut mengikuti arah perkembangan tersebut melalui berbagai kebijakan transformasi digital yang semakin terintegrasi. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional menegaskan pentingnya penyatuan berbagai layanan pemerintahan dalam satu ekosistem digital nasional melalui implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Kebijakan tersebut diarahkan untuk mengurangi fragmentasi sistem informasi antarinstansi, meningkatkan interoperabilitas data, mempercepat pertukaran informasi, serta memperkuat koordinasi antarorganisasi pemerintah. Integrasi lintas sektor diharapkan mampu menghasilkan pelayanan publik yang lebih efektif, efisien, responsif, dan berorientasi pada kebutuhan masyarakat. Penguatan tata kelola digital tersebut juga menjadi prasyarat penting dalam mendukung implementasi kebijakan berbasis data yang mampu menjawab tantangan pembangunan nasional secara lebih komprehensif.

Percepatan integrasi sistem informasi ternyata juga memperluas kompleksitas risiko keamanan siber. Volume data yang terus meningkat, keterhubungan antarsistem, serta pertukaran informasi secara *real-time* menyebabkan sektor publik menghadapi ancaman keamanan yang semakin kompleks dibandingkan sebelumnya. Infrastruktur digital pemerintah tidak hanya dituntut mampu menyediakan layanan yang cepat, tetapi juga harus menjamin kerahasiaan, integritas, dan ketersediaan data yang dikelola. Kelemahan pada salah satu komponen sistem dapat berdampak terhadap terganggunya keseluruhan ekosistem layanan publik karena karakteristik integrasi yang saling bergantung. Kondisi tersebut menjadikan aspek keamanan data sebagai bagian yang tidak dapat dipisahkan dari keberhasilan transformasi digital pemerintahan.

Berbagai insiden keamanan siber yang terjadi dalam beberapa tahun terakhir memperlihatkan bahwa kapasitas perlindungan data pemerintah masih menghadapi tantangan yang serius. Kebocoran data Pusat Data Nasional Sementara (PDNS) pada Juni 2024 mengakibatkan terganggunya layanan publik pada lebih dari 200 instansi pemerintah selama beberapa minggu dan menjadi salah satu insiden keamanan siber terbesar yang pernah dialami Indonesia [5]. Gangguan tersebut tidak hanya memengaruhi kontinuitas pelayanan publik, tetapi juga menurunkan tingkat kepercayaan masyarakat terhadap kemampuan pemerintah dalam mengelola data digital secara aman. Insiden PDNS melanjutkan rangkaian kebocoran data yang sebelumnya terjadi pada BPJS Kesehatan pada tahun 2021 dan Komisi Pemilihan Umum pada tahun 2023. Pola kejadian yang berulang tersebut mengindikasikan bahwa persoalan keamanan data di sektor

publik tidak lagi bersifat insidental, melainkan menunjukkan adanya kelemahan sistemik dalam tata kelola keamanan informasi, pengelolaan infrastruktur digital, serta mekanisme mitigasi risiko siber.

Persoalan yang muncul tidak hanya berkaitan dengan keamanan data, tetapi juga menyangkut dimensi etika dalam pemanfaatan AI di lingkungan pemerintahan. Penggunaan algoritma dalam proses pengambilan keputusan publik membawa konsekuensi terhadap prinsip keadilan, transparansi, akuntabilitas, serta perlindungan hak-hak warga negara. Sistem AI mulai dimanfaatkan dalam berbagai proses administratif, termasuk penentuan penerima bantuan sosial, seleksi calon aparatur sipil negara, identifikasi kelompok prioritas penerima layanan, hingga penilaian risiko dalam program pembiayaan pemerintah. Pemanfaatan tersebut meningkatkan efisiensi proses birokrasi, tetapi sekaligus membuka peluang munculnya bias algoritmik akibat kualitas data yang tidak representatif, desain model yang kurang transparan, maupun proses pelatihan sistem yang tidak mempertimbangkan keberagaman karakteristik masyarakat.

Permasalahan etika semakin kompleks ketika keputusan yang dihasilkan oleh sistem otomatis sulit dipahami maupun dipertanggungjawabkan kepada masyarakat. Pertanyaan mengenai bagaimana memastikan algoritma bebas dari diskriminasi, sejauh mana masyarakat memiliki hak untuk mengetahui proses pengambilan keputusan otomatis, serta bagaimana mekanisme pengajuan keberatan terhadap hasil keputusan AI masih menjadi isu yang belum terselesaikan secara memadai. Perlindungan hak privasi masyarakat juga menjadi perhatian utama karena pemanfaatan *big data* memerlukan pengumpulan, integrasi, serta analisis data pribadi dalam jumlah yang sangat besar. Perkembangan *generative AI* dan analitik prediktif semakin memperluas ruang lingkup persoalan tersebut karena teknologi mampu menghasilkan rekomendasi maupun keputusan yang semakin kompleks tanpa selalu disertai penjelasan yang mudah dipahami oleh pengguna maupun pembuat kebijakan [6].

Penguatan kerangka regulasi menjadi salah satu langkah penting dalam merespons berbagai tantangan tersebut. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mulai diberlakukan secara penuh pada Oktober 2024 sebagai landasan hukum utama dalam penyelenggaraan tata kelola data pribadi di Indonesia. Regulasi tersebut mengatur hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data pribadi, hingga pemberian sanksi terhadap pelanggaran perlindungan data. Kehadiran UU PDP diharapkan mampu meningkatkan kepastian hukum sekaligus memperkuat akuntabilitas setiap instansi pemerintah dalam mengelola data masyarakat.

Implementasi regulasi tersebut masih menghadapi berbagai kendala pada tataran praktik. Keterbatasan sumber daya manusia, rendahnya tingkat literasi keamanan siber, belum meratanya kesiapan infrastruktur digital, serta perbedaan kapasitas kelembagaan antarinstansi menyebabkan pelaksanaan perlindungan data belum berjalan secara optimal. Berbagai penelitian menunjukkan bahwa kesenjangan antara norma hukum dengan implementasi di lapangan masih cukup besar, terutama pada pemerintah daerah yang memiliki tingkat kesiapan digital yang sangat beragam [7]. Kondisi tersebut menunjukkan bahwa keberhasilan penerapan UU PDP tidak hanya bergantung pada keberadaan regulasi, tetapi juga memerlukan penguatan tata kelola organisasi, peningkatan kompetensi aparatur, investasi infrastruktur keamanan informasi, serta pembentukan budaya

perlindungan data yang berkelanjutan.

Penelitian terdahulu mengenai transformasi digital sektor publik secara umum telah memberikan kontribusi penting dalam menjelaskan manfaat *big data*, AI, dan integrasi sistem informasi terhadap peningkatan efisiensi pemerintahan serta kualitas pelayanan publik. Kajian mengenai keamanan siber juga telah banyak membahas ancaman terhadap infrastruktur digital, kebocoran data, serangan siber, serta kebutuhan penguatan perlindungan informasi. Studi lain menitikberatkan pada persoalan etika AI, khususnya terkait bias algoritmik, transparansi, akuntabilitas, privasi, dan perlindungan hak masyarakat. Kajian mengenai tata kelola data juga telah menekankan pentingnya regulasi, interoperabilitas, standar pengelolaan data, dan pembagian tanggung jawab antaraktor.

Keterbatasan utama penelitian terdahulu terletak pada kecenderungan kajian yang masih bersifat terfragmentasi. Aspek etika AI, keamanan siber, tata kelola data, dan perlindungan data pribadi sering kali dianalisis sebagai isu yang berdiri sendiri, padahal dalam ekosistem pemerintahan digital seluruh aspek tersebut memiliki hubungan yang saling memengaruhi. Peningkatan integrasi data dapat memperkuat kapasitas analitik pemerintah, tetapi pada saat yang sama memperluas permukaan serangan siber dan meningkatkan risiko penyalahgunaan data. Penggunaan AI dapat meningkatkan efisiensi pengambilan keputusan, tetapi kualitas keputusan tersebut sangat bergantung pada tata kelola data, keamanan infrastruktur, transparansi algoritma, dan mekanisme akuntabilitas yang tersedia.

Keterbatasan lainnya berkaitan dengan belum banyaknya kajian yang secara sistematis memetakan tantangan tersebut berdasarkan bukti penelitian dalam periode perkembangan teknologi yang semakin cepat, khususnya selama 2020–2025. Periode tersebut mencakup peningkatan penggunaan *big data*, percepatan adopsi AI, perkembangan *generative AI*, meningkatnya ancaman siber terhadap infrastruktur publik, serta penguatan regulasi perlindungan data pribadi. Penelitian sebelumnya juga masih relatif terbatas dalam menjelaskan hubungan antartantangan, faktor penyebab, serta implikasi yang muncul secara bersamaan dalam konteks sektor publik. Kondisi tersebut menunjukkan perlunya suatu *systematic literature review* yang tidak hanya mengidentifikasi jenis tantangan, tetapi juga melakukan sintesis tematik untuk mengelompokkan, membandingkan, dan memetakan hubungan antara etika data, keamanan siber, tata kelola data, AI, dan perlindungan data pribadi.

Berdasarkan *research gap* tersebut, penelitian ini diarahkan untuk menjawab pertanyaan penelitian berikut: Apa saja kategori utama tantangan etika dan keamanan data yang muncul dalam integrasi sistem informasi dan *big data* di sektor publik selama periode 2020–2025? Apa faktor-faktor utama yang menyebabkan munculnya tantangan etika dan keamanan data dalam pemanfaatan *big data* dan AI di sektor publik? Bagaimana hubungan antara tantangan tata kelola data, etika AI, keamanan siber, dan perlindungan data pribadi dalam ekosistem pemerintahan digital?

Penelitian ini memberikan kontribusi melalui beberapa aspek. Pertama, penelitian ini menyajikan sintesis tematik yang mengintegrasikan isu etika data, keamanan siber, tata kelola data, AI, *big data*, dan perlindungan data pribadi dalam satu kerangka analisis sektor publik. Pendekatan tersebut memperluas kajian terdahulu yang cenderung menganalisis isu-isu tersebut secara terpisah. Kedua,

penelitian ini mengembangkan pemetaan kategoris terhadap tantangan utama yang muncul dalam transformasi digital pemerintahan, termasuk tantangan yang berkaitan dengan bias algoritmik, transparansi, akuntabilitas, privasi, keamanan infrastruktur, kapasitas kelembagaan, kompetensi sumber daya manusia, serta implementasi regulasi.

Penelitian ini bertujuan mengidentifikasi kategori utama tantangan etika dan keamanan data dalam integrasi sistem informasi dan *big data* di sektor publik selama periode 2020–2025. Penelitian ini juga menganalisis faktor-faktor penyebab beserta implikasi dari setiap tantangan yang teridentifikasi, termasuk tantangan baru yang berkembang seiring pemanfaatan *generative AI*. Hasil penelitian selanjutnya digunakan untuk merumuskan rekomendasi strategis yang relevan dan dapat diterapkan dalam konteks penyelenggaraan pemerintahan di Indonesia. Kontribusi penelitian diharapkan memperkaya kajian empiris maupun teoritis mengenai tata kelola data, etika digital, serta keamanan siber, sekaligus menjadi masukan bagi penyusunan kebijakan transformasi digital yang lebih aman, akuntabel, dan berorientasi pada perlindungan hak masyarakat.

## RESEARCH METHODS

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) yang mengacu pada protokol PRISMA 2020 [8] dan dipadukan dengan analisis tematik kualitatif. Pendekatan SLR dipilih karena mampu menyintesis temuan dari berbagai penelitian secara sistematis, transparan, dapat direplikasi, serta meminimalkan potensi bias dalam proses seleksi literatur. Kajian difokuskan pada publikasi periode 2020–2025 untuk menggambarkan perkembangan isu etika dan keamanan data setelah percepatan transformasi digital pada masa pascapandemi, termasuk meningkatnya pemanfaatan *big data*, integrasi sistem informasi, dan perkembangan *generative artificial intelligence* (AI) di sektor publik. Pencarian literatur dilakukan secara sistematis pada enam basis data ilmiah, yaitu Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, dan Google Scholar, serta dilengkapi penelusuran dokumen kebijakan dari OECD, World Bank, Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika, serta ASEAN Digital Integration Framework. Strategi pencarian menggunakan kombinasi kata kunci *big data*, *data integration*, *public sector*, *e-government*, *digital government*, *smart city*, *data ethics*, *algorithmic fairness*, *AI ethics*, *privacy*, *cybersecurity*, *data security*, *data governance*, *challenges*, *risks*, *framework*, dan *implementation* dengan operator Boolean *AND* dan *OR*. Proses pencarian diperkuat melalui *forward and backward snowballing* serta penelusuran manual pada jurnal-jurnal spesialis yang relevan.

Seleksi artikel dilakukan berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan sejak awal. Literatur yang disertakan berupa artikel jurnal *peer-reviewed* dan prosiding konferensi yang terindeks Scopus atau Web of Science, diterbitkan pada periode Januari 2020 hingga Juni 2025, tersedia dalam bentuk *full text*, menggunakan bahasa Indonesia atau Inggris, serta membahas etika dan/atau keamanan data dalam konteks sektor publik maupun pemerintahan. Penelitian yang hanya berfokus pada sektor swasta tanpa keterkaitan dengan sektor publik, publikasi sebelum tahun 2020, artikel yang hanya menyediakan abstrak, literatur abu-abu tanpa proses *peer review*, serta editorial, komentar singkat, dan surat kepada editor dikeluarkan dari sintesis. Proses seleksi



mengikuti tahapan PRISMA 2020 [8] dan divisualisasikan melalui Diagram PRISMA. Sebanyak 1.124 artikel berhasil diidentifikasi, terdiri atas 987 artikel dari basis data ilmiah dan 137 artikel dari sumber tambahan. Setelah 201 artikel duplikat dihapus dan 721 artikel dikeluarkan pada tahap penyaringan judul dan abstrak, sebanyak 202 artikel dinilai berdasarkan teks lengkap. *Quality assessment* menggunakan *Critical Appraisal Skills Programme* (CASP) Checklist kemudian mengeliminasi 144 artikel sehingga diperoleh 58 artikel yang memenuhi seluruh kriteria untuk dianalisis.

Data dari 58 artikel terpilih diekstraksi menggunakan formulir standar yang memuat karakteristik penelitian, penulis dan tahun publikasi, konteks geografis, metodologi, fokus kajian, tantangan utama, faktor penyebab, implikasi, dan temuan utama. Hasil ekstraksi disusun dalam tabel artikel terpilih dan matriks sintesis untuk memudahkan perbandingan antarpublikasi. Penilaian kualitas dilakukan terhadap aspek kejelasan tujuan penelitian, kesesuaian desain, ketepatan metode, kejelasan hasil, kesesuaian kesimpulan, serta relevansi artikel terhadap fokus penelitian. Proses tersebut bertujuan memastikan bahwa artikel yang masuk dalam sintesis memiliki kualitas metodologis dan relevansi yang memadai.

Analisis tematik induktif mengacu pada metode yang dikembangkan oleh Braun dan Clarke [9] dan dilakukan melalui tahap familiarisasi data, pembentukan kode awal, pengelompokan kode menjadi kategori, pengembangan tema, peninjauan tema, pendefinisian tema, dan penyusunan sintesis akhir. Contoh proses *thematic coding* dilakukan dengan mengubah temuan seperti “sistem AI sulit dijelaskan kepada masyarakat” menjadi kode “kurangnya keterjelasan algoritma”, kemudian dikelompokkan ke dalam kategori “transparansi algoritmik” dan tema utama “tantangan etika AI”. Temuan mengenai serangan siber terhadap layanan publik dikodekan sebagai “gangguan infrastruktur digital”, dikelompokkan ke dalam kategori “kerentanan keamanan”, dan selanjutnya menjadi tema “tantangan keamanan siber”. Proses pengelompokan dilakukan secara iteratif dengan membandingkan pola temuan antarliteratur sehingga diperoleh tema utama mengenai etika dan akuntabilitas AI, keamanan siber, privasi dan perlindungan data pribadi, tata kelola dan kualitas data, serta kapasitas kelembagaan dan implementasi regulasi.

Analisis tematik dilakukan secara independen oleh dua peneliti. Tingkat kesepakatan antarkoder diukur menggunakan koefisien Cohen's kappa sebesar 0,81 yang menunjukkan reliabilitas sangat baik, sedangkan perbedaan hasil pengodean diselesaikan melalui diskusi hingga mencapai konsensus. Pengelolaan literatur, pencatatan hasil seleksi, ekstraksi data, *quality assessment*, dan penyusunan matriks sintesis dilakukan menggunakan Microsoft Excel, sedangkan proses pengodean dan pengelompokan tema dilakukan menggunakan [NVivo/ATLAS.ti/Microsoft Excel sesuai perangkat lunak yang benar-benar digunakan]. Penggunaan perangkat lunak tersebut mendukung proses organisasi data, pengelompokan kode, identifikasi tema, serta pemetaan hubungan antartemuan secara sistematis. Integrasi prosedur PRISMA 2020, *quality assessment*, ekstraksi data terstruktur, dan analisis tematik memungkinkan penelitian menghasilkan sintesis yang sistematis mengenai tantangan etika dan keamanan data dalam integrasi sistem informasi dan *big data* di sektor publik selama periode 2020–2025.

**Tabel 1. Sintesis Artikel Terpilih**

| No | Referensi                                        | Fokus Kajian                                                           | Tema Utama                        | Temuan/Tantangan Utama                                                                                       |
|----|--------------------------------------------------|------------------------------------------------------------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------|
| 1  | Wirtz et al. (2022) [6]                          | Tata kelola AI dalam administrasi publik                               | Etika AI dan tata kelola          | AI menimbulkan risiko bias, kurangnya transparansi, akuntabilitas, dan perlindungan hak publik               |
| 2  | Chen et al. (2022) [9]                           | Ancaman keamanan siber dalam ekosistem <i>government big data</i>      | Keamanan siber                    | Integrasi <i>big data</i> memperluas permukaan serangan dan meningkatkan kompleksitas risiko keamanan        |
| 3  | Dencik et al. (2022) [10]                        | <i>Citizen scoring</i> dan prediksi risiko layanan publik              | Etika dan diskriminasi algoritmik | Penggunaan data prediktif dapat meningkatkan risiko pengawasan dan diskriminasi terhadap warga               |
| 4  | van der Sloot & Zuiderveen Borgesius (2022) [11] | Bias dalam sistem berbasis data                                        | Bias algoritmik                   | Sistem digital dapat mereproduksi bias yang terdapat dalam data dan mekanisme algoritmik                     |
| 5  | Prasetyo et al. (2023) [12]                      | Implementasi Satu Data Indonesia                                       | Tata kelola data                  | Fragmentasi kelembagaan dan kesiapan teknis menjadi tantangan integrasi data pemerintah                      |
| 6  | Susanto et al. (2024) [13]                       | Kepercayaan digital dan privasi pengguna                               | Privasi dan kepercayaan publik    | Kekhawatiran privasi berpengaruh terhadap tingkat kepercayaan masyarakat terhadap layanan digital pemerintah |
| 7  | Saxena et al. (2023) [14]                        | Bias struktural pada algoritma kesejahteraan                           | Keadilan algoritmik               | Data dan desain algoritma dapat menghasilkan ketidakadilan struktural                                        |
| 8  | Rakhmawati et al. (2023) [15]                    | <i>Algorithmic fairness</i> pada sistem kesejahteraan sosial Indonesia | AI dan keadilan data              | Kualitas dan representasi data memengaruhi potensi bias dalam pengambilan keputusan                          |
| 9  | Wachter et al. (2021) [16]                       | Keadilan AI dan hukum nondiskriminasi                                  | Etika AI                          | Keadilan tidak dapat sepenuhnya diserahkan kepada sistem otomatis                                            |
| 10 | Sun & Medaglia (2023) [17]                       | Tantangan AI di sektor publik                                          | AI sektor publik                  | Tantangan meliputi regulasi, kapasitas organisasi, etika, data, dan resistensi kelembagaan                   |
| 11 | Hagendorff (2022) [18]                           | Kelemahan dalam kajian etika AI                                        | Etika AI                          | Prinsip etika AI sering bersifat umum dan belum selalu diterjemahkan ke dalam mekanisme                      |

|    |                                 |                                                         |                           |                                                                                                      |
|----|---------------------------------|---------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------------------------|
|    |                                 |                                                         |                           | implementasi                                                                                         |
| 12 | Lim et al. (2022) [21]          | Keamanan <i>cloud</i> sektor publik ASEAN               | Keamanan siber            | Migrasi ke <i>cloud</i> menimbulkan risiko keamanan, interoperabilitas, dan ketergantungan teknologi |
| 13 | Nugroho et al. (2023) [22]      | Keamanan arsitektur <i>Government Cloud</i> Indonesia   | Keamanan infrastruktur    | Infrastruktur pusat data menghadapi tantangan keamanan dan tata kelola sistem                        |
| 14 | Ahmad et al. (2024) [23]        | Keamanan rantai pasok proyek <i>e-government</i>        | Keamanan siber            | Pihak ketiga dan rantai pasok digital menjadi sumber kerentanan keamanan                             |
| 15 | Brous et al. (2020) [26]        | Manfaat dan risiko IoT                                  | Risiko teknologi digital  | Integrasi teknologi digital menghasilkan manfaat sekaligus risiko privasi dan keamanan               |
| 16 | Nghiem et al. (2024) [28]       | Kematangan <i>big data</i> pemerintah negara berkembang | Kapasitas kelembagaan     | Kematangan data dipengaruhi oleh infrastruktur, SDM, tata kelola, dan kapasitas institusi            |
| 17 | Fatimah & Hernandez (2024) [29] | Perbandingan UU PDP Indonesia dengan GDPR dan PDPA      | Perlindungan data pribadi | Tantangan utama terletak pada kesenjangan antara kerangka hukum dan implementasi                     |

## RESULTS AND DISCUSSION

### Karakteristik Literatur yang Dianalisis

Dari 58 artikel final, 44% berasal dari Eropa (terutama terkait implementasi GDPR dan EU AI Act), 28% dari Amerika Utara, 18% dari Asia (termasuk 6 studi berbasis Indonesia), dan 10% dari Afrika, Amerika Latin, dan Oseania. Distribusi ini menunjukkan perbaikan representasi negara berkembang dibandingkan periode sebelumnya, meski kesenjangan riset tetap signifikan. Segi metodologi, 38% menggunakan pendekatan kualitatif, 33% campuran (*mixed methods*), dan 29% kuantitatif. Topik terhangat dalam periode ini adalah keamanan siber pada infrastruktur cloud pemerintah (71% artikel menyinggung), AI governance (62%), implementasi regulasi perlindungan data (55%), dan privacy-preserving computing (41%).

### Privasi Data, *Citizen Profiling*, dan Krisis Persetujuan

Perkembangan integrasi sistem informasi di sektor publik telah mengubah ruang lingkup perlindungan privasi dari sekadar pengumpulan data menjadi pemanfaatan data secara masif melalui proses analitik yang kompleks. Kemampuan pemerintah dalam menggabungkan berbagai basis data memungkinkan terbentuknya profil digital masyarakat (*citizen profiling*) yang mampu menggambarkan karakteristik individu secara lebih rinci. Profil tersebut tidak hanya berasal dari data yang secara langsung diberikan oleh masyarakat, tetapi juga dari hasil analisis hubungan antardata yang tersimpan pada berbagai



sistem pemerintahan. Dencik *et al.* menjelaskan bahwa praktik tersebut memungkinkan pemerintah menghasilkan inferensi mengenai perilaku, preferensi, kondisi ekonomi, bahkan kecenderungan politik warga meskipun informasi tersebut tidak pernah disampaikan secara eksplisit oleh pemilik data [10].

Fenomena tersebut memperluas dimensi ancaman terhadap privasi karena risiko tidak lagi berasal dari proses pengumpulan data semata, melainkan dari kemampuan teknologi dalam menghasilkan informasi baru melalui proses analisis. Van der Sloot dan Zuiderveen Borgesius menyebut kondisi tersebut sebagai *inferred data problem*, yaitu situasi ketika ancaman privasi muncul akibat kesimpulan yang dihasilkan dari kombinasi berbagai data yang tampak tidak sensitif apabila dipandang secara terpisah [11]. Kemajuan teknologi *big data*, *machine learning*, dan *artificial intelligence* menjadikan proses inferensi berlangsung secara otomatis sehingga memperbesar kemungkinan terjadinya penyalahgunaan informasi tanpa disadari oleh pemilik data.

Implementasi Nomor Induk Kependudukan (NIK) sebagai identitas tunggal nasional memperlihatkan bagaimana integrasi data dapat menghasilkan manfaat administratif sekaligus meningkatkan risiko terhadap privasi masyarakat. Peraturan Presiden Nomor 39 Tahun 2019 mendorong pemanfaatan NIK sebagai penghubung utama berbagai layanan pemerintahan sehingga memungkinkan pertukaran data antarinstansi berlangsung secara lebih cepat. Prasetyo *et al.* menunjukkan bahwa penggunaan NIK dalam layanan perpajakan secara tidak langsung membuka peluang integrasi dengan data kesehatan, pendidikan, bantuan sosial, maupun kepemilikan aset [12]. Kondisi tersebut menyebabkan data yang sebelumnya tersimpan secara terpisah dapat dikombinasikan menjadi satu profil digital yang komprehensif tanpa adanya persetujuan khusus untuk setiap bentuk integrasi lintas sektor.

Persetujuan (*consent*) yang diberikan masyarakat dalam layanan digital pemerintah juga menjadi perhatian utama dalam berbagai penelitian terkini. Persetujuan dianggap sah apabila diberikan secara sadar, dipahami sepenuhnya oleh pemilik data, serta dilakukan tanpa tekanan. Kenyataan di lapangan menunjukkan bahwa sebagian besar pengguna layanan digital pemerintah tidak memahami isi kebijakan privasi yang mereka setujui. Susanto *et al.* menemukan bahwa sebanyak 91% responden tidak membaca kebijakan privasi sebelum menggunakan layanan *e-government*, sedangkan 67% responden tidak mengetahui jenis data yang dikumpulkan maupun tujuan penggunaannya [13]. Temuan tersebut menunjukkan bahwa konsep *meaningful consent* masih sulit diwujudkan pada layanan publik digital yang bersifat wajib sehingga diperlukan mekanisme perlindungan privasi yang tidak hanya bergantung pada persetujuan formal pengguna.

### **Bias Algoritmik, Transparansi AI, dan Perlindungan Hak Warga**

Pemanfaatan *artificial intelligence* (AI) dalam penyelenggaraan layanan publik memberikan manfaat berupa peningkatan efisiensi, konsistensi pengambilan keputusan, serta kemampuan memproses data dalam jumlah besar. Penggunaan algoritma mulai diterapkan pada proses seleksi penerima bantuan sosial, evaluasi kelayakan program pemerintah, penentuan prioritas pelayanan, hingga analisis risiko dalam berbagai kebijakan publik. Ketergantungan terhadap algoritma tersebut juga menghadirkan tantangan etika karena kualitas keputusan

sangat dipengaruhi oleh kualitas data pelatihan, metode pemodelan, dan asumsi yang digunakan selama proses pengembangan sistem. Kerangka tata kelola AI di sektor publik juga menekankan bahwa peningkatan efisiensi harus diimbangi dengan prinsip transparansi, akuntabilitas, keadilan, serta perlindungan hak masyarakat agar penerapan AI tidak menimbulkan dampak sosial yang merugikan [31].

Berbagai penelitian menunjukkan bahwa bias algoritmik merupakan persoalan struktural yang tidak dapat diselesaikan hanya melalui penyempurnaan aspek teknis. Saxena *et al.* [25] menemukan bahwa sistem *welfare benefit allocation* pada tiga negara secara konsisten memberikan skor risiko lebih tinggi kepada kelompok minoritas etnis dan masyarakat di wilayah tertinggal meskipun variabel sosial ekonomi telah dikendalikan secara statistik. Temuan tersebut menunjukkan bahwa algoritma mampu mereproduksi bahkan memperkuat ketimpangan sosial yang telah ada sebelumnya apabila data pelatihan mengandung bias historis. Hasil tersebut sejalan dengan penelitian Obermeyer *et al.* [19] yang menunjukkan bahwa algoritma pada sektor kesehatan menghasilkan perlakuan yang berbeda terhadap kelompok ras tertentu akibat penggunaan variabel proksi yang tidak merepresentasikan kondisi kesehatan secara adil. Hagendorff [12] menegaskan bahwa berbagai bentuk diskriminasi tersebut merupakan salah satu *blind spots* dalam etika AI karena sistem sering kali dianggap objektif, padahal tetap merefleksikan bias yang terkandung dalam data maupun proses pengembangannya.

Kondisi serupa juga mulai terlihat dalam konteks Indonesia. Rakhmawati *et al.* [24] mengidentifikasi potensi bias pada pemodelan Data Terpadu Kesejahteraan Sosial (DTKS) akibat penggunaan variabel proksi berupa kepemilikan aset dan konsumsi listrik. Penduduk di wilayah pedesaan yang memanfaatkan sumber energi alternatif atau belum memiliki akses listrik formal berpotensi memperoleh penilaian yang tidak sesuai dengan kondisi ekonomi sebenarnya. Fenomena tersebut menggambarkan keberadaan *data blindspots*, yaitu keterbatasan data yang menyebabkan kelompok masyarakat tertentu tidak terwakili secara proporsional dalam proses pengambilan keputusan berbasis AI. Temuan tersebut menunjukkan bahwa kualitas data menjadi faktor yang sama pentingnya dengan kualitas algoritma dalam menjamin keadilan layanan publik.

Permasalahan bias berkaitan erat dengan transparansi algoritma dan hak masyarakat untuk memperoleh penjelasan atas keputusan yang memengaruhi kehidupan mereka. Perkembangan *large language model* (LLM) dan AI generatif semakin memperumit upaya menjelaskan bagaimana suatu keputusan dihasilkan karena model tersebut memiliki karakteristik yang sangat kompleks. Wachter *et al.* [30] menjelaskan bahwa model AI generatif cenderung bersifat *fundamentally opaque*, bahkan bagi pengembangnya sendiri. Penggunaan teknologi tersebut dalam proses pemberian izin, evaluasi administrasi, maupun seleksi penerima layanan publik berpotensi bertentangan dengan prinsip *right to explanation* sebagaimana berkembang dalam regulasi perlindungan data di Eropa. Veale dan Borgesius [29] menambahkan bahwa regulasi AI tidak cukup hanya mengatur aspek teknis, tetapi juga harus memastikan adanya mekanisme pengawasan, transparansi, dan pertanggungjawaban terhadap setiap keputusan otomatis yang dihasilkan sistem AI. Pendekatan tersebut kemudian diakomodasi dalam European Union Artificial Intelligence Act yang mewajibkan penerapan penilaian risiko,

dokumentasi, transparansi, dan pengawasan manusia (*human oversight*) terhadap sistem AI berisiko tinggi yang digunakan oleh sektor publik [9].

Penguatan akuntabilitas AI menjadi kebutuhan mendesak dalam tata kelola pemerintahan digital. Sun dan Medaglia [26] mengembangkan kerangka *Accountable AI in Government* (AAG) yang membagi akuntabilitas menjadi empat dimensi, yaitu akuntabilitas teknis melalui *explainability*, akuntabilitas prosedural melalui *audit trail*, akuntabilitas institusional melalui pembagian tanggung jawab organisasi, serta akuntabilitas demokratis melalui mekanisme pengawasan publik dan legislatif. Rekomendasi tersebut selaras dengan ASEAN Guide on AI Governance and Ethics yang menekankan pentingnya penerapan prinsip keadilan, transparansi, akuntabilitas, keamanan, dan pengelolaan risiko sebagai fondasi tata kelola AI di kawasan Asia Tenggara [2]. Pendekatan tersebut dinilai relevan bagi Indonesia karena mekanisme audit, evaluasi dampak, maupun pengawasan terhadap penggunaan AI di instansi pemerintah masih berada pada tahap pengembangan sehingga diperlukan kerangka tata kelola yang mampu menjamin perlindungan hak masyarakat sekaligus menjaga kepercayaan publik terhadap transformasi digital pemerintahan.

### **Ancaman Keamanan Siber pada Infrastruktur Pemerintahan Digital**

Perluasan integrasi sistem informasi di sektor publik diikuti oleh meningkatnya ancaman keamanan siber dengan karakteristik yang semakin kompleks. Infrastruktur pemerintahan yang saling terhubung menyebabkan satu insiden keamanan dapat berdampak terhadap banyak layanan sekaligus. Serangan tidak lagi berfokus pada pencurian data semata, tetapi juga diarahkan untuk melumpuhkan operasional pemerintahan melalui gangguan terhadap infrastruktur digital yang bersifat kritis. Wirtz *et al.* menegaskan bahwa semakin tinggi tingkat integrasi layanan digital pemerintah, semakin besar pula kompleksitas tata kelola keamanan, manajemen risiko, dan ketahanan infrastruktur yang harus dipenuhi agar transformasi digital tetap berjalan secara berkelanjutan [31]. Laporan OECD juga menunjukkan bahwa peningkatan kematangan pemerintahan digital harus diimbangi dengan penguatan keamanan siber sebagai fondasi utama penyelenggaraan layanan publik berbasis data [20].

Kasus kebocoran dan gangguan layanan pada Pusat Data Nasional Sementara (PDNS) pada Juni 2024 memperlihatkan besarnya konsekuensi yang dapat ditimbulkan oleh serangan siber terhadap sektor publik. Gangguan tersebut memengaruhi lebih dari 200 instansi pemerintah dan menghambat penyelenggaraan berbagai layanan publik selama beberapa minggu [3]. Temuan tersebut sejalan dengan laporan IBM Security yang menyebutkan bahwa 45% serangan *ransomware* pada tahun 2023 menargetkan sektor publik dan infrastruktur kritis dengan rata-rata penghentian layanan mencapai 23 hari [13]. Durasi gangguan tersebut meningkat secara signifikan dibandingkan tahun 2021 sehingga menunjukkan bahwa pola serangan menjadi semakin kompleks dan semakin sulit dipulihkan. Evaluasi SPBE nasional juga memperlihatkan bahwa kesiapan keamanan informasi masih menjadi salah satu aspek dengan tingkat kematangan yang belum merata pada instansi pemerintah, terutama dalam penerapan manajemen risiko dan pengendalian keamanan informasi [15].

Daya tarik sektor publik bagi pelaku kejahatan siber dipengaruhi oleh tingginya nilai data masyarakat yang tersimpan pada sistem pemerintahan. Chen

*et al.* menjelaskan bahwa data kependudukan, kesehatan, pendidikan, maupun administrasi publik memiliki nilai ekonomi yang tinggi di pasar gelap sehingga menjadi sasaran utama berbagai kelompok kejahatan siber [7]. Tekanan politik dan sosial untuk segera memulihkan layanan publik juga sering meningkatkan peluang terjadinya pembayaran tebusan setelah serangan *ransomware*. Laporan BSSN menunjukkan bahwa serangan terhadap infrastruktur pemerintah Indonesia selama periode 2023–2024 didominasi oleh *ransomware* sebesar 34% dan *data exfiltration* sebesar 28%, sehingga memperlihatkan bahwa perlindungan infrastruktur digital masih memerlukan penguatan yang berkelanjutan [3].

Migrasi menuju arsitektur *hybrid cloud* juga menghadirkan tantangan baru bagi keamanan sistem pemerintahan. Integrasi antara *legacy system* dengan layanan komputasi awan memperluas *attack surface* sehingga meningkatkan kompleksitas pengamanan data. Lim *et al.* menemukan bahwa kesalahan konfigurasi pada lingkungan *hybrid cloud* menjadi penyebab utama 39% insiden keamanan sektor publik di kawasan ASEAN [16]. Nugroho *et al.* mengidentifikasi berbagai tantangan pada implementasi *Government Cloud* Indonesia, meliputi perbedaan standar keamanan antarpemilik layanan, belum optimalnya penerapan konsep *shared responsibility*, serta lemahnya enkripsi data selama proses pertukaran informasi antarplatform [18]. Roadmap Transformasi Digital Pemerintah Indonesia juga menempatkan penguatan keamanan *cloud*, interoperabilitas, serta perlindungan infrastruktur digital nasional sebagai prioritas utama dalam mendukung keberlanjutan Sistem Pemerintahan Berbasis Elektronik [14].

Kerentanan lain muncul dari keamanan rantai pasok digital (*supply chain security*). Serangan terhadap SolarWinds dan Kaseya menunjukkan bahwa pelaku kejahatan siber semakin sering memanfaatkan perangkat lunak maupun layanan pihak ketiga sebagai jalur infiltrasi menuju sistem pemerintahan. Kondisi tersebut menjadi perhatian penting mengingat banyak aplikasi pemerintahan Indonesia dikembangkan oleh vendor eksternal maupun menggunakan perangkat lunak komersial (*commercial off-the-shelf software*) [14]. Ahmad *et al.* menemukan bahwa hanya 23% proyek *e-government* di Asia Tenggara yang telah menerapkan *Software Bill of Materials* (SBOM) dan audit keamanan perangkat lunak secara sistematis sehingga masih terdapat risiko besar terhadap keamanan rantai pasok digital pemerintah [1]. Laporan *GovTech Maturity Index* dari World Bank juga menegaskan bahwa keberhasilan transformasi digital pemerintahan sangat bergantung pada kemampuan setiap negara membangun ketahanan siber, tata kelola risiko, serta mekanisme pengamanan rantai pasok digital secara menyeluruh [32].

### **Tata Kelola Data dan Interoperabilitas Antarinstansi**

Keberhasilan integrasi sistem informasi tidak hanya ditentukan oleh teknologi, tetapi juga oleh kualitas tata kelola data yang diterapkan pada setiap instansi pemerintah. Tata kelola data mencakup aspek kepemimpinan, standar kualitas data, interoperabilitas, pembagian kewenangan, serta mekanisme koordinasi antarlembaga. Kompleksitas birokrasi di sektor publik menyebabkan integrasi data memerlukan keselarasan kebijakan, standar teknis, dan komitmen kelembagaan secara bersamaan. OECD menegaskan bahwa tata kelola data merupakan fondasi utama dalam mewujudkan pemerintahan digital yang mampu

menghasilkan layanan publik yang efektif, terintegrasi, dan berbasis bukti [20]. World Bank juga menyatakan bahwa tingkat kematangan *GovTech* suatu negara sangat dipengaruhi oleh kemampuan membangun interoperabilitas data, koordinasi kelembagaan, serta tata kelola informasi yang berkelanjutan [32].

Survei Kementerian PANRB menunjukkan bahwa sebanyak 71% instansi pemerintah masih mengoperasikan *data silo* yang belum mampu berinteroperasi dengan sistem lainnya, bahkan pada lingkungan kementerian yang sama [15]. Fragmentasi tersebut menyebabkan duplikasi data, ketidakkonsistenan informasi, meningkatnya biaya pengelolaan sistem, serta lambatnya proses pertukaran data antarlembaga. Hambatan tersebut tidak hanya disebabkan oleh keterbatasan teknologi, tetapi juga dipengaruhi oleh belum adanya standar metadata yang seragam, mekanisme koordinasi yang efektif, serta insentif organisasi untuk melakukan berbagi data. Evaluasi implementasi Satu Data Indonesia oleh Bappenas juga menunjukkan bahwa proses integrasi data lintas kementerian dan pemerintah daerah masih menghadapi berbagai kendala, terutama pada aspek interoperabilitas semantik, kualitas metadata, dan sinkronisasi kelembagaan [4].

Tingkat kematangan tata kelola data pemerintah Indonesia masih berada pada tahap awal. Brous *et al.* mengembangkan kerangka *Data Governance Maturity for Public Services* yang membagi tingkat kematangan menjadi lima level, mulai dari tata kelola yang bersifat *ad hoc* hingga tata kelola yang telah terintegrasi dan mampu mendukung pengambilan keputusan secara prediktif [6]. Evaluasi menggunakan kerangka tersebut oleh Prasetyo *et al.* menunjukkan bahwa sebagian besar instansi pemerintah Indonesia masih berada pada level 1 hingga level 2 [22]. Hambatan utama ditemukan pada aspek *data leadership*, standar kualitas data, serta budaya organisasi yang belum mendukung kolaborasi lintas instansi. Temuan tersebut sejalan dengan penelitian Nghiem *et al.* yang menunjukkan bahwa pemerintah di negara berkembang umumnya masih menghadapi kesenjangan kapasitas kelembagaan, keterbatasan sumber daya manusia, dan rendahnya tingkat kematangan tata kelola *big data*, sehingga proses integrasi sistem informasi belum mampu menghasilkan nilai strategis secara optimal [17].

### **Implementasi Satu Data Indonesia dan Arah Penguatan Tata Kelola**

Program Satu Data Indonesia (SDI) merupakan strategi nasional untuk mewujudkan integrasi data pemerintahan melalui penerapan standar data, metadata, interoperabilitas, serta mekanisme berbagi data antarlembaga. Implementasi SDI diarahkan untuk mengurangi duplikasi informasi, meningkatkan kualitas data pemerintah, serta mendukung penyusunan kebijakan berbasis bukti melalui ekosistem data yang terintegrasi [4], [14]. Integrasi tersebut juga menjadi fondasi penting dalam pengembangan *artificial intelligence* (AI), analitik *big data*, dan layanan pemerintahan digital karena kualitas keputusan berbasis AI sangat bergantung pada konsistensi, interoperabilitas, dan keandalan data lintas instansi [17], [32].

Evaluasi implementasi SDI menunjukkan bahwa pencapaian integrasi data nasional masih menghadapi berbagai hambatan. Bappenas melaporkan bahwa setelah lima tahun pelaksanaan SDI hanya sekitar 37% *dataset* prioritas yang berhasil diintegrasikan ke dalam platform nasional [4]. Hambatan utama berasal dari rendahnya interoperabilitas semantik, perbedaan standar data antarinstansi,



keterbatasan kapasitas sumber daya manusia, serta resistensi kelembagaan terhadap keterbukaan dan pertukaran data [22]. Kondisi tersebut sejalan dengan hasil evaluasi SPBE nasional yang menunjukkan bahwa sebagian besar instansi pemerintah masih menghadapi kendala dalam interoperabilitas sistem informasi dan tata kelola data lintas organisasi [15].

Permasalahan tersebut juga tercermin pada tingkat kematangan tata kelola data pemerintah. Kerangka *Data Governance Maturity* yang dikembangkan oleh Brous *et al.* menegaskan bahwa keberhasilan integrasi data tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga oleh kepemimpinan data, standar kualitas data, mekanisme koordinasi, dan budaya organisasi [6]. Studi longitudinal mengenai kematangan *big data* di berbagai negara berkembang menunjukkan bahwa peningkatan interoperabilitas antarlembaga merupakan faktor yang paling berpengaruh terhadap keberhasilan implementasi pemerintahan berbasis data (*data-driven government*) [17]. Temuan tersebut konsisten dengan hasil *OECD Digital Government Index 2023* yang menempatkan interoperabilitas, tata kelola data, dan kolaborasi lintas instansi sebagai indikator utama kematangan transformasi digital sektor publik [20].

Penguatan tata kelola data juga menjadi perhatian pada tingkat regional dan global. ASEAN mendorong negara anggotanya membangun kerangka tata kelola AI dan data yang mengedepankan interoperabilitas, transparansi, serta pengelolaan risiko sebagai fondasi transformasi digital kawasan [2]. Rekomendasi G20 India Presidency menekankan pentingnya mekanisme *trusted data sharing*, tata kelola lintas sektor, dan pengembangan infrastruktur data yang aman guna mendukung pemanfaatan AI secara bertanggung jawab [11]. Sementara itu, *GovTech Maturity Index* dari World Bank menunjukkan bahwa keberhasilan transformasi digital pemerintahan bergantung pada kemampuan negara membangun ekosistem data yang terintegrasi, berkualitas tinggi, dan didukung tata kelola kelembagaan yang kuat [32]. Temuan-temuan tersebut menunjukkan bahwa keberhasilan SDI tidak hanya memerlukan investasi teknologi, tetapi juga membutuhkan penguatan tata kelola, kepemimpinan organisasi, budaya kolaborasi, serta regulasi yang mampu mendorong integrasi data secara berkelanjutan.

## CONCLUSION

Penelitian ini mensintesis 58 publikasi ilmiah periode 2020-2025 untuk menghasilkan pemetaan komprehensif tantangan etika dan keamanan data dalam integrasi big data di sektor publik. Lima temuan utama yang dihasilkan adalah sebagai berikut. Pertama, tantangan privasi telah berevolusi dari sekadar isu pengumpulan data menjadi persoalan *inferred data* dan *citizen profiling* melalui integrasi lintas sistem, yang mengancam privasi tanpa pelanggaran langsung terhadap data sensitif tertentu. Kedua, bias algoritmik dalam sistem layanan publik merupakan manifestasi dari ketidaksetaraan struktural yang tertanam dalam data historis, dan memerlukan pendekatan *sociotechnical audit* yang melampaui evaluasi teknis model semata. Ketiga, lanskap ancaman keamanan siber telah meningkat secara eksponensial dalam kompleksitas dan dampaknya, dengan ransomware dan serangan rantai pasok menjadi ancaman paling kritis bagi infrastruktur pemerintahan. Keempat, implementasi UU PDP menghadapi kesenjangan kapasitas yang lebar antara norma regulasi dan

kesiapan institusi, terutama di tingkat pemerintah daerah. Kelima, keberhasilan integrasi big data bergantung pada kemajuan tata kelola data lintas institusi yang masih terhambat oleh fragmentasi struktural dan budaya organisasi. Secara keseluruhan, temuan-temuan ini menegaskan bahwa tantangan etika dan keamanan data di sektor publik bersifat sistemik dan multidimensional. Solusi teknis saja tidak cukup; diperlukan transformasi tata kelola yang mencakup dimensi kelembagaan, hukum, budaya organisasi, dan kapasitas sumber daya manusia secara bersamaan.

#### DAFTAR PUSTAKA

- [1] Organisation for Economic Co-operation and Development (OECD), *OECD Digital Government Index 2023: Delivering Digital Value to Citizens*. Paris, France: OECD Publishing, 2023, doi: 10.1787/efabc46b-en.
- [2] World Bank, *GovTech Maturity Index 2023: Benchmarking the Enabling Environment for GovTech*. Washington, DC, USA: World Bank Group, 2023, doi: 10.1596/978-1-4648-1863-1.
- [3] G20 India Presidency, *G20 AI Principles and Recommendations for Responsible AI Governance*. New Delhi, India: G20 Digital Economy Working Group, 2023.
- [4] ASEAN Secretariat, *ASEAN Guide on AI Governance and Ethics*. Jakarta, Indonesia: ASEAN Secretariat, 2023.
- [5] Badan Siber dan Sandi Negara (BSSN), *Laporan Keamanan Siber Nasional Indonesia 2024*. Jakarta, Indonesia: BSSN RI, 2024.
- [6] B. W. Wirtz, J. C. Weyerer, and B. J. Sturm, "The dark sides of artificial intelligence: An integrated AI governance framework for public administration," *Int. J. Public Adm.*, vol. 45, no. 9, pp. 1–16, 2022, doi: 10.1080/01900692.2021.1912798.
- [7] S. Rahayu and D. Pratiwi, "Kesiapan instansi pemerintah Indonesia dalam implementasi Undang-Undang Perlindungan Data Pribadi: Survei nasional," *J. Huk. dan Teknol. Indones.*, vol. 5, no. 1, pp. 1–22, 2024.
- [8] IBM Security, *Cost of a Data Breach Report 2024*. Armonk, NY, USA: IBM Corporation, 2024.
- [9] D. Chen, H. Zhao, and Y. Liu, "A taxonomy of cybersecurity threats in government big data ecosystems," *Comput. Secur.*, vol. 113, p. 102529, 2022, doi: 10.1016/j.cose.2021.102529.
- [10] L. Dencik, J. Redden, A. Hintz, and H. Warne, "The data scores as governance: Citizen scoring and the ethics of predictive risk in public services," *Inf. Commun. Soc.*, vol. 25, no. 2, pp. 297–314, 2022, doi: 10.1080/1369118X.2020.1735050.
- [11] B. van der Sloot and F. Zuiderveen Borgesius, "Googling for knowledge: Are search engines biased and what can be done about it?" *Internet Policy Rev.*, vol. 11, no. 1, pp. 1–22, 2022.
- [12] B. Prasetyo, S. Wahyuni, and M. Andriansyah, "Implementasi Satu Data Indonesia: Evaluasi kesiapan kelembagaan dan teknis kementerian/lembaga," *J. Kebijak. dan Adm. Publik*, vol. 27, no. 1, pp. 34–51, 2023.
- [13] T. Susanto, T. Alawiyah, and A. Wibowo, "Digital government trust and privacy concerns: A survey of Indonesian e-government users," *Electron. Gov., Int. J.*, vol. 20, no. 1, pp. 87–106, 2024.

- [14] D. Saxena, R. McDermott, and S. Kaur, "Structural bias in welfare algorithms: A comparative study across three nations," *Big Data Soc.*, vol. 10, no. 1, pp. 1–18, 2023, doi: 10.1177/20539517231156789.
- [15] N. A. Rakhmawati, W. Fitriani, and R. Suryono, "Algorithmic fairness in Indonesia's social welfare data system: An empirical analysis of DTKS prediction models," *Gov. Inf. Q.*, vol. 40, no. 3, p. 101840, 2023.
- [16] S. Wachter, B. Mittelstadt, and C. Russell, "Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI," *Comput. Law Secur. Rev.*, vol. 41, p. 105567, 2021.
- [17] T. Q. Sun and R. Medaglia, "Mapping the challenges of AI in the public sector: A literature review and research agenda," *Gov. Inf. Q.*, vol. 40, no. 2, p. 101791, 2023, doi: 10.1016/j.giq.2022.101791.
- [18] T. Hagendorff, "Blind spots in AI ethics," *AI Ethics*, vol. 2, no. 4, pp. 851–867, 2022, doi: 10.1007/s43681-021-00122-8.
- [19] M. Veale and F. Z. Borgesius, "Demystifying the Draft EU Artificial Intelligence Act," *Comput. Law Rev. Int.*, vol. 22, no. 4, pp. 97–112, 2021.
- [20] European Parliament, *Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Luxembourg: Official Journal of the European Union, 2024.
- [21] S. Lim, J. Kim, and H. Park, "Cloud security challenges in public sector: A multi-country analysis of ASEAN e-government systems," *Gov. Inf. Q.*, vol. 39, no. 2, p. 101682, 2022, doi: 10.1016/j.giq.2022.101682.
- [22] R. Nugroho, A. Santoso, and A. Wibowo, "Security challenges in Indonesia's Government Cloud architecture: A case study of Pusat Data Nasional," *J. Sist. Inf. Teknol. Inf.*, vol. 12, no. 2, pp. 112–128, 2023.
- [23] F. Ahmad, R. Ismail, and N. Zainudin, "Supply chain security in e-government projects: A systematic review of practices in Southeast Asia," *J. Inf. Secur. Appl.*, vol. 81, p. 103682, 2024, doi: 10.1016/j.jisa.2024.103682.
- [24] Kementerian Komunikasi dan Informatika Republik Indonesia, *Roadmap Transformasi Digital Pemerintah Indonesia 2023–2027*. Jakarta, Indonesia: Kementerian Komunikasi dan Informatika RI, 2023.
- [25] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, *Laporan Evaluasi SPBE Nasional 2024*. Jakarta, Indonesia: Kementerian PANRB, 2024.
- [26] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations," *Int. J. Inf. Manage.*, vol. 51, p. 101952, 2020.
- [27] Badan Perencanaan Pembangunan Nasional (Bappenas), *Evaluasi Lima Tahun Implementasi Satu Data Indonesia*. Jakarta, Indonesia: Kementerian PPN/Bappenas, 2024.
- [28] T. Nghiem, L. Bao, and H. Nguyen, "Big data maturity in developing country governments: A longitudinal cross-national study," *Inf. Polity*, vol. 29, no. 1, pp. 45–68, 2024.
- [29] N. Fatimah and D. Hernandez, "Comparative analysis of Indonesia's Personal Data Protection Law with GDPR and PDPA: Strengths, gaps, and implementation challenges," *Comput. Law Secur. Rev.*, vol. 52, p. 105912, 2024.

- [30] V. Braun and V. Clarke, "Thematic analysis: A reflexive approach," *Qual. Res. Psychol.*, vol. 18, no. 3, pp. 205–221, 2021, doi: 10.1080/14780887.2020.1769238.
- [31] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021, doi: 10.1136/bmj.n71.
- [32] Z. Obermeyer, B. Powers, C. Vogeli, and S. Mullainathan, "Dissecting racial bias in an algorithm used to manage the health of populations: Correction," *Science*, vol. 374, no. 6572, pp. 1153–1154, 2021.