Jurnal kedaulatan hukum

Vol. [2] Masalah [1], [2026] Diisi oleh Redaksi Pelaksana
E-ISSN 3123-6790
Jurnal Terakreditasi Nasional,
DOI: Diisi oleh Managing Editor

Konstitusi dan Keamanan Siber Layanan Publik: Kekosongan Regulasi AI sebagai Ancaman terhadap Hak atas Rasa Aman dan Perlindungan Data Pribadi

Intan Erniyasari[1], Aurelia Rahmadita Putri[2], Linda Widianti [3], Ricky Arisandi[4]

[123]Fakultas Hukum dan Ilmu Sosial, [4]Fakultas Sains dan Teknologi,
[123]Universitas Muhammadiyah Kotabumi, [4]Universitas Islam Negeri Raden Intan Lampung
aureliarahmaditaputri3@gmail.com, intan.erniyasari0502@gmail.com, lwidianti287@gmail.com, rickyarisandi2004@gmail.com

ABSTRACT

This article examines the constitutional implications of deploying artificial intelligence (AI) in Indonesian public services from the perspectives of cybersecurity and personal data protection. While digital public services may improve efficiency and responsiveness, the increasing use of AI systems also expands cybersecurity risks, amplifies large-scale personal data processing, and creates accountability gaps when algorithmic outputs affect administrative actions. This study aims to analyze how the regulatory vacuum on AI governance can threaten the constitutional right to a sense of security and weaken personal data protection in public service delivery, and to propose a legally accountable regulatory direction. Using a normative legal method with a statute approach and a conceptual approach, the research analyzes constitutional principles, relevant statutory frameworks on electronic systems and data protection, and legal concepts of transparency, accountability, and state responsibility. The findings indicate that existing rules remain fragmented and are not sufficiently specific to regulate AI-related obligations such as risk assessment, auditability, minimum transparency/explainability, human oversight for high-impact decisions, and effective remedies for citizens harmed by data breaches or erroneous automated outcomes. Therefore, the article recommends a risk-based AI governance framework for public services that integrates cybersecurity safeguards, clear liability allocation, incident response standards, and accessible mechanisms for objections and redress to ensure constitutional compliance in the digital era.

Keywords: Artificial Intelligence; Constitutional Rights; Cybersecurity; Personal Data Protection; Public Services

Pendahuluan

Hak atas rasa aman dan perlindungan data pribadi menjadi semakin menentukan ketika layanan publik bergeser ke sistem digital yang mengandalkan pengolahan data warga. Di satu sisi, digitalisasi mempercepat pelayanan dan membuka ruang inovasi berbasis data, tetapi di sisi lain ia memperluas risiko ketika data sensitif diproses lintas aplikasi, vendor, dan infrastruktur. Dalam konteks negara hukum, kemajuan teknologi seharusnya tidak mengurangi kewajiban negara untuk memastikan layanan publik berjalan aman, dapat dipercaya, dan tidak

menimbulkan kerugian bagi warga. Perlindungan ini tidak berhenti pada "ada tidaknya layanan", melainkan juga pada bagaimana negara mencegah penyalahgunaan data serta menyediakan mekanisme koreksi ketika warga dirugikan. Karena itu, isu keamanan siber dan tata kelola data bukan sekadar persoalan teknis, melainkan bagian dari pemenuhan hak konstitusional warga dalam praktik administrasi negara modern. Sejalan dengan itu, penguatan pelindungan data juga terkait langsung dengan tantangan penerapan UU PDP yang masih menghadapi hambatan kelembagaan dan implementasi (Syailendra, 2024).

Kerentanan layanan publik digital terlihat jelas ketika instansi bergantung pada pihak ketiga, terutama penyedia layanan infrastruktur awan (*cloud*) dan pengelola sistem. Ketergantungan ini sering membuat titik risiko berpindah dari "aplikasi pemerintah" menjadi "rantai layanan" yang melibatkan vendor, kontrak, serta pengaturan akses dan pemrosesan data. Dalam salah satu evaluasi menggunakan Indeks Keamanan Informasi (KAMI), aspek pengamanan keterlibatan pihak ketiga hanya mencapai 49% dan pengamanan layanan infrastruktur awan 33%, sementara area perlindungan data pribadi berada pada 67%, yang menunjukkan masih adanya celah serius pada tata kelola keamanan layanan berbasis *cloud* (Hafizuddin & Sugiantoro, 2024).

Indeks KAMI dalam literatur juga dipahami sebagai salah satu alat penilaian keamanan informasi yang disusun/diadopsi dalam ekosistem tata kelola keamanan informasi nasional dan dipakai untuk melihat kesiapan pengamanan organisasi. Pada artikel yang sama, Indeks KAMI dijelaskan sebagai alat penilaian yang disusun oleh Kementerian Komunikasi dan Informatika, serta penggunaan versi 4.2 didasarkan pada SNI ISO. Kondisi seperti ini relevan bagi layanan publik karena kebocoran atau gangguan layanan tidak hanya berdampak pada sistem, tetapi juga pada keselamatan digital warga yang datanya dikelola oleh negara. Dengan demikian, fakta sosialnya adalah: perluasan layanan publik digital tanpa ketahanan keamanan yang memadai dapat menggeser risiko menjadi ancaman nyata bagi rasa aman dan perlindungan data (Hafizuddin & Sugiantoro, 2024)

Perkembangan berikutnya adalah pemanfaatan kecerdasan buatan (AI) yang mulai masuk ke proses layanan publik, baik untuk otomasi, analisis, maupun pengambilan keputusan berbasis rekomendasi sistem. AI dalam layanan publik dapat dipahami sebagai penggunaan model algoritmik untuk memproses data dan menghasilkan keluaran yang memengaruhi tindakan administratif, misalnya klasifikasi permohonan, prioritisasi layanan, atau pemantauan tertentu. Literatur tentang integrasi AI dalam administrasi publik menekankan bahwa efisiensi perlu diimbangi dengan akuntabilitas, ketahanan, dan pengaturan risiko agar keputusan yang dipengaruhi AI tetap dapat dipertanggungjawabkan (Vatamanu & Tofan, 2025). Pada konteks Indonesia, AI di layanan publik juga sering dibaca sebagai peluang meningkatkan efisiensi, tetapi tetap menuntut perhatian serius pada isu privasi dan arah kebijakan teknologi agar penerapannya tidak memunculkan masalah baru (Komarudin et al., 2025).

Kekosongan regulasi AI menjadi problem ketika layanan publik berbasis AI beroperasi dalam ekosistem siber yang risikonya terus berkembang dan lintas batas. Di banyak kasus, kerangka hukum yang ada belum cukup spesifik untuk menjawab

pertanyaan “batas penggunaan AI”, “standar transparansi keputusan”, dan “siapa bertanggung jawab ketika sistem merugikan warga”. Ketika sistem AI sulit dijelaskan (*black-box*) dan proses pengambilan keputusan tidak transparan, akuntabilitas bisa melemah karena warga tidak mengetahui dasar keputusan, sedangkan negara berpotensi kehilangan jejak pertanggungjawaban. Kajian tentang transparansi dan akuntabilitas AI menegaskan bahwa lemahnya dua aspek ini dapat berdampak serius pada kesejahteraan individu/masyarakat, karena sistem yang sulit diaudit membuat kontrol hukum dan sosial menjadi tidak efektif (Cheong, 2024). Selain itu, AI juga menghadirkan “risiko siber baru” karena dapat dimanfaatkan untuk serangan yang lebih canggih dan sekaligus membuat sistem AI menjadi target serangan (*adversarial attacks*), sehingga memperbesar ancaman pada layanan digital (Vulpe et al., 2024)

Beberapa risiko utama yang relevan dalam konteks layanan publik berbasis AI antara lain:

1. Pelanggaran perlindungan data, ketika data warga diproses besar-besaran tanpa transparansi yang memadai, atau keamanan penyimpanan dan pertukaran datanya lemah (Syailendra, 2024)
2. Peningkatan ancaman keamanan siber, baik karena AI dapat memperkuat kemampuan penyerang maupun karena sistem AI dapat diserang/diakali sehingga keputusan layanan menjadi salah atau berbahaya (Vulpe et al., 2024).
3. Celah akuntabilitas administrasi, ketika keputusan sistem tidak dapat dijelaskan dan tidak jelas siapa yang bertanggung jawab secara hukum atas kerugian warga (Cheong, 2024)

Kebaruan kajian ini terletak pada pembingkaian kekosongan regulasi AI bukan hanya sebagai masalah kebijakan teknologi, tetapi sebagai ancaman konstitusional terhadap hak atas rasa aman dan perlindungan data dalam layanan publik. Studi tentang AI dalam administrasi publik banyak menekankan aspek manfaat–tantangan tata kelola secara umum, tetapi belum selalu menempatkan kekosongan aturan AI sebagai sumber kerentanan yang langsung menguji akuntabilitas negara dalam layanan publik (Komarudin et al., 2025; Vatamanu & Tofan, 2025). Kajian tentang AI dan keamanan siber juga memperlihatkan karakter risiko AI yang kompleks dan berdampak pada kepercayaan publik, namun belum cukup menajamkan implikasi yuridisnya pada pemulihan hak warga ketika dirugikan oleh layanan publik berbasis AI (Vulpe et al., 2024). Di sisi lain, pembahasan UU PDP menyoroti tantangan implementasi perlindungan data, namun belum mengikatnya secara tegas pada praktik AI sebagai sumber risiko tambahan yang menuntut standar tata kelola khusus di layanan publik (Syailendra, 2024). Karena itu, artikel ini bertujuan menganalisis kebutuhan pengaturan AI yang selaras dengan nilai konstitusi dan prinsip hukum administrasi negara, terutama untuk memastikan keamanan siber layanan publik, kepastian akuntabilitas, dan perlindungan data pribadi warga di tengah ketiadaan regulasi AI yang komprehensif.

Metode

Penelitian ini bertujuan menganalisis kekosongan regulasi AI dalam layanan publik dari perspektif konstitusi dan hukum administrasi negara, khususnya terkait hak atas rasa aman dan perlindungan data pribadi, serta merumuskan arah pengaturan yang lebih akuntabel. Metode yang digunakan adalah yuridis-normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konseptual, sehingga hasil diperoleh melalui penelaahan norma tertulis dan penguatan analisis konsep/prinsip hukum yang relevan. Data penelitian berupa data sekunder yang dikumpulkan melalui studi pustaka, meliputi bahan hukum primer (UUD NRI 1945 dan peraturan perundang-undangan terkait sistem elektronik, keamanan siber, serta perlindungan data), bahan hukum sekunder (literatur hukum, artikel jurnal, dan hasil penelitian terdahulu), serta bahan hukum tersier (kamus hukum, ensiklopedia, dan sumber penunjang). Seluruh data dianalisis secara kualitatif dengan penalaran hukum yang sistematis melalui inventarisasi norma, interpretasi, dan konstruksi argumentasi untuk menilai kecukupan pengaturan yang ada dan menyusun rekomendasi kerangka regulasi AI yang selaras dengan prinsip konstitusional serta akuntabilitas penyelenggaraan layanan publik digital.

Diskusi

Temuan kajian ini menunjukkan bahwa pemanfaatan AI dalam layanan publik Indonesia berjalan lebih cepat dibanding kesiapan kerangka pengaturan yang mampu memastikan keamanan sistem, perlindungan data, dan akuntabilitas keputusan administratif. Pada level prinsip, hak atas rasa aman dan perlindungan data/privasi dapat ditautkan dengan jaminan konstitusional (khususnya Pasal 28G ayat (1) UUD 1945) dan kemudian dioperasionalkan melalui rezim perlindungan data (UU PDP) yang masih menghadapi tantangan implementasi(Syailendra, 2024). Di sisi lain, penelitian-penelitian keamanan informasi pada sistem layanan berbasis *cloud* menunjukkan adanya celah nyata pada pengamanan pihak ketiga dan infrastruktur, yang berarti risiko warga sering justru muncul dari rantai layanan, bukan hanya dari aplikasi pemerintahnya. Ketika AI ditambahkan ke dalam ekosistem tersebut (otomasi, klasifikasi, rekomendasi keputusan), maka risiko yang semula teknis dapat berubah menjadi persoalan hukum administrasi negara: warga bisa terdampak oleh keputusan yang sulit dijelaskan, sulit diaudit, dan sulit dipulihkan ketika terjadi kesalahan atau kebocoran(Hafizuddin & Sugiantoro, 2024).

Selain itu, pemanfaatan AI di sektor publik juga sering diposisikan sebagai instrumen untuk memperkuat akuntabilitas dan kepercayaan publik, misalnya melalui peningkatan transparansi proses, penguatan pengawasan, dan perbaikan kualitas pengambilan keputusan berbasis data. Namun, literatur menegaskan bahwa dampak positif tersebut hanya realistis bila AI ditempatkan dalam kerangka tata kelola yang jelas mulai dari penetapan tujuan yang sah, pengendalian risiko, hingga mekanisme pertanggungjawaban ketika sistem menimbulkan kerugian atau salah output. Dalam konteks itu, AI bukan sekadar alat teknis, tetapi bagian dari

desain institusional yang harus selaras dengan nilai demokratis dan etika pemerintahan, termasuk memastikan adanya kontrol manusia dan prosedur koreksi. Ketika standar-standar tersebut tidak tersedia atau tidak seragam, penggunaan AI justru berpotensi memperbesar *accountability gap* karena publik kesulitan menelusuri proses, memverifikasi keluaran, dan menuntut pemulihan secara efektif. Karena itu, diskusi mengenai kekosongan regulasi AI perlu dipertegas sebagai masalah tata kelola sektor publik yang berkaitan langsung dengan perlindungan hak dan akuntabilitas penyelenggara layanan (Aldemir & Uçma Uysal, 2025).

Pembahasan

1. Hak atas rasa aman dan perlindungan data dalam layanan publik digital

Peralihan layanan publik ke sistem digital menempatkan data warga sebagai "bahan baku" utama, sehingga kualitas perlindungan data menentukan kualitas perlindungan hak. UU PDP dipandang sebagai kemajuan penting, tetapi berbagai studi menekankan bahwa hambatan implementasi (kesiapan kelembagaan, kepatuhan pengendali/pemroses data, dan penegakan) berpotensi membuat perlindungan hak berjalan tidak merata(Syailendra, 2024). Pada saat yang sama, kajian politik hukum UU PDP mengaitkan perlindungan data dengan hak atas privasi sebagai hak dasar yang dijamin konstitusi, sehingga kelalaian dalam pengelolaan data layanan publik dapat dipahami sebagai masalah pemenuhan hak, bukan sekadar ketidaktertiban administrasi(Fauzi et al., 2022) . Dalam kerangka ini, "rasa aman" tidak hanya bermakna aman fisik, tetapi juga aman dari penyalahgunaan identitas, pemerasan digital, profiling yang tidak sah, maupun kerugian akibat kebocoran data. Karena itu, isu keamanan siber layanan publik perlu diposisikan sebagai bagian dari kewajiban negara untuk memastikan layanan yang tertib, dapat dipercaya, dan melindungi warga.

Pemanfaatan AI dalam e-government juga perlu dibaca dari sisi penerimaan dan kepercayaan warga, karena layanan publik yang "cerdas" tetap akan dipakai dan dinilai publik melalui persepsi manfaat, risiko, dan rasa aman. Tinjauan sistematis tentang pergeseran dari e-government ke AI-enabled e-government menunjukkan bahwa sikap warga dipengaruhi oleh faktor seperti persepsi kegunaan, kemudahan, tingkat kepercayaan, serta kekhawatiran atas privasi dan risiko yang melekat pada sistem AI (Savveli et al., 2025). Pada saat yang sama, kajian open access di Heliyon menekankan bahwa integrasi AI (termasuk ketika dipadukan dengan teknologi digital lain) memang dapat meningkatkan transparansi, akuntabilitas, dan efisiensi layanan, tetapi manfaat itu sangat bergantung pada desain tata kelola dan kontrol risikonya sejak awal(Al-Ansi et al., 2024). Artinya, regulasi AI dalam layanan publik tidak cukup berhenti pada "boleh atau tidak", melainkan harus menjamin standar operasional yang membuat warga paham bagaimana sistem bekerja, bagaimana datanya diproses, dan jalur apa yang tersedia ketika terjadi kesalahan. Jika standar tersebut tidak ada, kepercayaan publik mudah runtuh karena warga melihat AI sebagai sistem yang "memutuskan sendiri" tanpa penjelasan dan tanpa pertanggungjawaban yang jelas. Karena itu, kekosongan regulasi AI berpotensi

memperbesar jarak antara tujuan modernisasi layanan dan pengalaman warga, karena inovasi yang tidak diiringi jaminan keamanan dan perlindungan data justru memperkuat persepsi risiko dan menurunkan legitimasi layanan publik digital.

2. Kerentanan keamanan siber layanan publik dan risiko AI

Studi evaluasi keamanan informasi pada penyedia layanan *cloud* dan perlindungan data pribadi dengan Indeks KAMI menunjukkan bahwa titik rawan sering berada pada pengamanan pihak ketiga dan layanan infrastruktur awan, yang mengindikasikan masih kuatnya *supply-chain risk* dalam ekosistem layanan digital(Hafizuddin & Sugiantoro, 2024). Dalam praktik layanan publik, ketergantungan pada vendor dan integrasi lintas sistem membuat satu kelemahan dapat merembet menjadi kegagalan layanan atau kebocoran data skala besar. Pada kondisi ini, AI dapat memperluas permukaan risiko karena AI bergantung pada data besar, integrasi sistem, dan proses otomatis yang berjalan cepat. Literatur tentang AI di administrasi publik menekankan bahwa manfaat efisiensi AI harus diimbangi dengan tata kelola risiko, ketahanan sistem, dan kontrol yang memadai agar layanan tetap akuntabel (Vatamanu & Tofan, 2025). Dengan kata lain, tanpa standar keamanan dan tata kelola yang jelas, AI dapat mengubah problem keamanan siber menjadi problem konstitusional: negara berpotensi gagal memastikan perlindungan hak ketika layanan berbasis AI menimbulkan kerugian.

2.1 Pelanggaran perlindungan data dan *data governance* yang lemah

AI cenderung mendorong pengumpulan, pemrosesan, dan pertukaran data dalam skala yang lebih luas; kondisi ini meningkatkan risiko pelanggaran privasi bila transparansi, dasar pemrosesan, dan pengamanan data tidak kuat. Tantangan implementasi UU PDP yang dicatat dalam studi Indonesia Law Review memperlihatkan bahwa perlindungan data membutuhkan kesiapan institusional dan kepatuhan yang konsisten agar hak subjek data tidak berhenti di atas kertas (Syailendra, 2024). Pada saat yang sama, kajian keamanan informasi berbasis ISO 27001 dan Indeks KAMI menekankan pentingnya tata kelola sistem manajemen keamanan informasi (ISMS) sebagai fondasi pengendalian risiko kebocoran dan pelanggaran keamanan (Apriany & Wibowo, 2024). Artinya, jika AI digunakan untuk layanan publik tetapi organisasi belum matang dalam manajemen keamanan informasi, maka "inovasi" justru dapat memperbesar peluang pelanggaran data warga.

2.2 Ancaman keamanan siber terhadap AI dan penggunaan AI untuk serangan

AI tidak hanya "membutuhkan keamanan", tetapi juga dapat menjadi bagian dari ancaman: ia dapat dimanfaatkan penyerang untuk meningkatkan skala/ketepatan serangan, sekaligus AI itu sendiri dapat menjadi target serangan (*adversarial attacks*) yang mengubah keluaran sistem. Riset Frontiers menunjukkan bahwa relasi AI–keamanan siber semakin kompleks: AI dapat memperkuat pertahanan, tetapi juga menciptakan vektor ancaman baru dan tantangan privasi (Putra et al., 2024). Dalam layanan publik, serangan semacam ini dapat berdampak ganda mengganggu ketersediaan layanan sekaligus mengganggu integritas keputusan (misalnya keluaran rekomendasi/klasifikasi yang salah). Oleh sebab itu, "keamanan siber layanan publik" tidak cukup dimaknai sebagai keamanan jaringan,

tetapi juga keamanan model, data pelatihan, dan rantai pasok teknologi yang menopang AI.

2.3 Celah akuntabilitas keputusan administratif berbasis AI

Masalah kunci dalam layanan publik berbasis AI adalah risiko *accountability gap*: ketika keputusan atau rekomendasi sistem menimbulkan dampak negatif, warga sulit menelusuri alasan keputusan dan sulit menentukan siapa yang bertanggung jawab. Kajian tentang transparansi dan akuntabilitas AI menegaskan bahwa sistem yang tidak transparan dan sulit diaudit berpotensi melemahkan mekanisme kontrol sosial maupun kontrol hukum (Jassinta & Erliyana, 2025). Dalam konteks hukum administrasi negara, situasi ini berbahaya karena keputusan layanan publik seharusnya memenuhi prinsip keterbukaan, dapat diuji, dan menyediakan ruang keberatan/banding yang efektif. Jika AI digunakan tanpa standar penjelasan keputusan, dokumentasi proses, dan *human oversight*, maka warga berisiko kehilangan akses pada "alasan" dan "pemulihan", padahal keduanya adalah inti perlindungan hukum dalam pelayanan publik.

3. Kekosongan regulasi AI sebagai masalah hukum administrasi negara

Kekosongan regulasi AI tidak selalu berarti "tidak ada aturan sama sekali", tetapi sering berupa ketiadaan standar operasional yang spesifik: klasifikasi risiko, kewajiban audit, kewajiban transparansi, batas penggunaan, dan skema tanggung jawab ketika terjadi kerugian. Kajian di Notaire menyoroti tantangan pengaturan AI di Indonesia dalam perspektif konseptual, termasuk problem penentuan subjek/pertanggungjawaban dan kebutuhan desain regulasi yang mampu mengikuti perkembangan teknologi (Ravizki & Lintang Yudhantaka, 2022). Pada ranah kebijakan publik, penelitian tentang implementasi AI dalam tata kelola publik Indonesia juga menyinggung bahwa penggunaan AI membawa isu keamanan data dan tantangan implementasi yang memerlukan kesiapan tata Kelola (Agustian et al., 2025). Dengan demikian, kekosongan regulasi AI dapat dibaca sebagai "kekosongan perlindungan" ketika AI dipakai pada layanan publik: aturan umum mungkin ada (UU ITE/UU PDP), tetapi standar khusus untuk AI yang mengunci keamanan, transparansi, dan akuntabilitas belum cukup tegas dan seragam.

Penting juga ditegaskan bahwa pemanfaatan AI dalam layanan publik pada praktiknya tidak berdiri sendiri, melainkan melekat pada kerangka Sistem Pemerintahan Berbasis Elektronik (SPBE) yang sejak awal memang mendorong penggunaan teknologi baru termasuk *big data*, *IoT,* dan *artificial intelligence* untuk pengelolaan data warga dan peningkatan layanan, ketika SPBE mengandalkan pemrosesan data secara masif, sementara pengaturan perlindungan data pada level undang-undang masih tersebar dan tidak seragam, maka ruang abu-abu penggunaan AI berpotensi memperbesar risiko pelanggaran privasi, *security incident*, dan sengketa administrasi karena standar operasionalnya tidak terkunci dengan jelas (Rahman, 2021). Dari sisi tata kelola, penguatan regulasi AI seharusnya tidak berhenti pada larangan atau imbauan etis, tetapi dibangun sebagai mekanisme akuntabilitas yang konkret misalnya standar pengumpulan/transfer data, kewajiban pelaporan insiden pelanggaran data, serta skema sanksi dan kompensasi yang dapat dipulihkan melalui prosedur hukum, studi kebijakan di

Indonesia juga menekankan urgensi pembentukan otoritas pelindungan data yang terpusat agar pengawasan pemrosesan data (termasuk dalam ekosistem AI) tidak tercecer antar-instansi dan bisa dipertanggungjawabkan secara kelembagaan (Badriah et al., 2024). Dengan kerangka seperti ini, kekosongan regulasi AI dapat dipetakan sebagai "celah akuntabilitas administrasi": negara tetap menyelenggarakan layanan digital, tetapi instrumen pengendalian risiko dan pemulihan hak warga belum cukup kuat untuk menjamin rasa aman serta perlindungan data secara efektif.

4. Implikasi: AI yang tidak diatur memperbesar risiko terhadap hak atas rasa aman

Jika layanan publik memanfaatkan AI tanpa kerangka pengaturan yang memadai, maka risiko yang muncul bukan hanya kebocoran data, tetapi juga risiko ketidakadilan administratif, keputusan yang tidak dapat dijelaskan, serta lemahnya jalur pemulihan bagi warga. Studi tentang AI di administrasi publik menekankan bahwa integrasi AI seharusnya memperkuat ketahanan dan kualitas tata kelola, bukan menciptakan kerentanan baru (Vatamanu & Tofan, 2025). Sementara itu, penelitian keamanan informasi menunjukkan bahwa organisasi perlu memastikan kematangan pengamanan dan tata kelola (misalnya melalui ISMS/ISO 27001 dan evaluasi kematangan) sebelum memperluas pemrosesan data dan integrasi sistem yang lebih kompleks (Apriany & Wibowo, 2024). Karena itu, kekosongan regulasi AI dalam layanan publik patut diposisikan sebagai ancaman terhadap hak atas rasa aman dan perlindungan data: bukan karena AI "pasti salah", tetapi karena tanpa standar yang mengikat, negara berisiko kehilangan kemampuan mencegah, mengendalikan, dan memulihkan kerugian warga secara adil.

Ketimpangan tata kelola keamanan ini juga tercermin pada praktik layanan publik yang sudah lebih dulu mengandalkan integrasi basis data lintas institusi. Studi pada layanan pemeriksaan imigrasi menunjukkan bahwa kebijakan sistem terintegrasi (antara basis data Interpol dan sistem manajemen perbatasan) belum berjalan optimal karena antara lain minimnya landasan hukum pelaksanaan, keterbatasan kapasitas SDM, keterbatasan jaringan/basis data, sampai keterbatasan keamanan platform; dampaknya bukan hanya memperlambat layanan, tetapi juga berpotensi memunculkan risiko keamanan yang lebih besar (Ryanindityo et al., 2025). Dalam konteks layanan publik yang mulai menambahkan AI untuk klasifikasi, deteksi, dan rekomendasi, kondisi "integrasi data yang belum matang" seperti ini dapat memperlebar ruang masalah: AI akan memproses data yang mengalir lintas sistem, sehingga bila dasar hukumnya lemah dan kontrol keamanannya minim, maka potensi pelanggaran hak atas rasa aman dan perlindungan data menjadi makin sulit dicegah sekaligus makin sulit dipulihkan secara administratif.

Dari sisi kebijakan, isu tersebut sejalan dengan temuan kajian hukum siber yang menilai serangan terhadap infrastruktur pemerintah (misalnya kasus PDNS) memperlihatkan bahwa konstruksi hukum siber Indonesia masih lemah karena belum ada regulasi yang khusus dan komprehensif, sehingga perlu desain reformasi yang mencakup pembentukan UU siber, harmonisasi aturan sektoral, penguatan pengawasan demokratis, pelibatan multi-stakeholder, dan perlindungan hak digital

warga (Wijaya et al., 2025). Pada saat yang sama, kajian mengenai keamanan siber dan kedaulatan data juga menekankan bahwa dominasi pendekatan "state-centered" belum otomatis mewujudkan kedaulatan data dan proteksi data pribadi; kapasitas dan kapabilitas warga (people-centered) tetap penting untuk menjaga data di ruang siber (Hidayat & Radyawanto, 2025). Karena itu, kekosongan regulasi AI dalam layanan publik semestinya dibaca sebagai problem administrasi negara yang nyata: tanpa standar yang mengikat (keamanan, auditabilitas, akuntabilitas keputusan algoritmik, dan mekanisme keberatan/pemulihan), negara berisiko gagal memenuhi kewajiban konstitusionalnya dalam menjamin rasa aman serta melindungi data pribadi warga dalam pelayanan publik digital.

Kesimpulan

Pemanfaatan AI dalam layanan publik mempercepat proses pelayanan, namun sekaligus memperbesar risiko terhadap hak atas rasa aman dan perlindungan data pribadi ketika diterapkan dalam ekosistem digital yang masih memiliki celah keamanan dan tata kelola. Masalah utama yang ditemukan adalah kekosongan regulasi AI yang membuat standar operasional seperti uji risiko, auditabilitas, transparansi keputusan, human oversight, serta pembagian tanggung jawab belum terkunci secara tegas, padahal AI dapat menghasilkan keputusan yang sulit dijelaskan (black-box). Kondisi ini diperparah oleh ketergantungan layanan publik pada pihak ketiga dan infrastruktur cloud, sehingga insiden keamanan atau kebocoran data sering muncul dari "rantai layanan", bukan hanya dari aplikasi pemerintah. Ketika terjadi gangguan atau keputusan AI yang keliru, mekanisme koreksi dan pemulihan hak warga berisiko tidak efektif karena akuntabilitas sulit ditelusuri dan standar pembuktian tidak jelas. Dengan demikian, kekosongan pengaturan AI bekerja melalui mekanisme "celah akuntabilitas" dan "celah keamanan" yang pada akhirnya dapat menggerus perlindungan hak konstitusional warga dalam layanan publik digital.

Rekomendasi utama artikel ini adalah perlunya kerangka pengaturan AI layanan publik yang berbasis risiko dan terintegrasi dengan rezim keamanan siber serta perlindungan data, mencakup kewajiban penilaian risiko sebelum implementasi, audit dan dokumentasi sistem, transparansi minimum yang dapat dipahami warga, pengawasan manusia pada keputusan berdampak tinggi, serta prosedur keberatan/pemulihan dan pertanggungjawaban yang jelas ketika terjadi kerugian. Selain itu, penguatan tata kelola perlu dilakukan melalui standardisasi keamanan (misalnya penguatan ISMS, manajemen vendor, dan respons insiden), serta harmonisasi aturan sektoral agar tidak terjadi tumpang tindih maupun kekosongan kewenangan. Keterbatasan penelitian ini terletak pada metodologi yang bersifat yuridis-normatif berbasis data sekunder, sehingga belum menguji langsung praktik implementasi AI di instansi tertentu, belum memetakan variasi kesiapan antar lembaga, dan belum menilai aspek teknis keamanan model AI secara mendalam. Karena itu, penelitian lanjutan disarankan menggunakan pendekatan empiris (wawancara, studi kasus instansi, dan analisis insiden) untuk menguji efektivitas mekanisme pemulihan hak warga serta menilai kebutuhan standar teknis yang lebih operasional dalam regulasi AI layanan publik.

Referensi

Agustian, D., Regif, S. Y., Hironimus Botha, H., Pattipeilohy, A. & Ode, S. (2025). Artificial Intelligence in The Implementation of Public Governance: Public Data Security Vulnerabilities in Indonesia. In *Jurnal Kebijakan Publik* | (Vol. 16, Issue 1). http://jkp.ejournal.unri.ac.id

Al-Ansi, A. M., Garad, A., Jaboob, M. & Al-Ansi, A. (2024). Elevating e-government: Unleashing the power of AI and IoT for enhanced public services. In *Heliyon* (Vol. 10, Issue 23). Elsevier Ltd. https://doi.org/10.1016/j.heliyon.2024.e40591

Aldemir, C. & Uçma Uysal, T. (2025). Artificial Intelligence for Financial Accountability and Governance in the Public Sector: Strategic Opportunities and Challenges. *Administrative Sciences*, *15*(2). https://doi.org/10.3390/admsci15020058

Apriany, A. & Wibowo, A. (2024). Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *18*(4). https://doi.org/10.22146/ijccs.100385

Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*, *6*. https://doi.org/10.3389/numd.2024.1421273

Badriah, L., Indiahono, D. & Sukarso. (2024). Akuntabilitas dalam Kebijakan Perlindungan Data Pribadi di Indonesia Accountability in Personal Data Protection Policy in Indonesia Learning from South Korea and Singapore. *Jurnal Inovasi Kebijakan*, *8*(2), 89–102. https://doi.org/10.21787/mp.8.2.2024.89-102

Fauzi, E., Alif, N. & Shandy, R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Renaissance*.

Hafizuddin, F. A. & Sugiantoro, B. (2024). Evaluasi Keamanan Sistem Informasi Pada Penyedia Layanan Cloud Dan Perlindungan Data Pribadi Berdasarkan Index Kami Versi 4.2 (Studi Kasus : PTIPD UIN Sunan Kalijaga Yogyakarta). *CyberSecurity Dan Forensik Digital*, *7*(1), 7–17.

Hidayat, S. & Radyawanto, S. A. (2025). KEMANDIRIAN SIBER INDONESIA: TANTANGAN DAN PELUANG MENUJU KEDAULATAN DIGITAL. *INTERNATIONAL JOURNAL OF SOCIAL AND MANAGEMENT STUDIES (IJOSMAS)*. https://www.ijosmas.org

Jassinta, M. A. P. & Erliyana, A. (2025). Keabsahan Keputusan Tata Usaha Negara yang Berlaku Retroaktif (Studi Kasus Surat Keputusan Menteri Dalam Negeri

Tentang Pemberhentian Sementara Wakil Bupati Mimika). *Lex Renaissance*, *10*(1), 222–248. https://doi.org/10.20885/jlr.vol10.iss1.art9

Komarudin, D., Baharuddin, M. & Tjenreng, Z. (2025). PERAN KECERDASAN BUATAN DALAM MENINGKATKAN EFISIENSI PELAYANAN PUBLIK DI INDONESIA. In *Jurnal Ilmiah Ilmu Pemerintahan* (Vol. 11, Issue 2).

Putra, E. A. M., Wibowo, G. D. H. & Minollah, M. (2024). Legal Vacuum in Indonesian Administrative Law: Urgency of Policy Regulation. *Indonesian Journal of Law and Economics Review*, *19*(1). https://doi.org/10.21070/ijler.v19i1.991

Rahman, F. (2021). KERANGKA HUKUM PERLINDUNGAN DATA PRIBADI DALAM PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI INDONESIA. *Jurnal LEGISLASI INDONESIA*.

Ravizki, E. N. & Lintang Yudhantaka. (2022). Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia. *Notaire*, *5*(3), 351–376. https://doi.org/10.20473/ntr.v5i3.39063

Ryanindityo, M., Aji, K. P., Briando, B. & Syahrin, M. A. (2025). Transformasi Digital untuk Meningkatkan Layanan dan Keamanan di Tempat Pemeriksaan Imigrasi di Indonesia: Studi Terhadap Kebijakan Basis Data Terintegrasi. *Jurnal Administrasi Publik*, *21*(1), 1–31. https://doi.org/10.52316/jap.v21i1.429

Savveli, I., Rigou, M. & Balaskas, S. (2025). From E-Government to AI E-Government: A Systematic Review of Citizen Attitudes. In *Informatics* (Vol. 12, Issue 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/informatics12030098

Syailendra, M. R. (2024). PERSONAL DATA PROTECTION LAW IN INDONESIA: CHALLENGES AND OPPORTUNITIES. *Indonesia Law Review*, *14*(2). https://doi.org/10.15742/ilrev.v14n2.4

Vatamanu, A. F. & Tofan, M. (2025). Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. *Administrative Sciences*, *15*(4). https://doi.org/10.3390/admsci15040149

Vulpe, S. N., Rughiniș, R., Țurcanu, D. & Rosner, D. (2024). AI and cybersecurity: a risk society perspective. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1462250

Wijaya, C. T., Sujadmiko, B. & Zazili, A. (2025). Efektivitas Perlindungan Hukum Terhadap Peretasan Data Di Pusat Data Nasional. *JUSTICIA SAINS: JURNAL ILMU HUKUM*. https://doi.org/10.24967/jcs.v10i2.4217