ISSN 2621- 458X

DIGITAL IDENTITY DAN AUTHENTICATION MECHANISM DALAM PELAYANAN PEMERINTAHAN DIGITAL: STUDI PERLINDUNGAN DATA PENGGUNA DI KABUPATEN BARRU

Hendra

Program Studi Magister Administrasi Publik, ITBA Al Gazali Barru

Hendrahendrabarru@gmail.com

ABSTRAK

Transformasi digital pemerintahan mendorong implementasi identitas digital sebagai fondasi utama penyelenggaraan layanan publik berbasis elektronik. Namun, efektivitas implementasi identitas digital di tingkat pemerintah daerah masih menghadapi berbagai tantangan, terutama terkait mekanisme autentikasi, perlindungan data pribadi, dan kesiapan kelembagaan. Penelitian ini bertujuan menganalisis implementasi identitas digital di Kabupaten Barru, mengevaluasi efektivitas mekanisme autentikasi yang digunakan, mengidentifikasi kesenjangan antara regulasi dan praktik perlindungan data, serta merumuskan rekomendasi kebijakan untuk memperkuat tata kelola identitas digital. Penelitian menggunakan pendekatan kualitatif deskriptif melalui studi kepustakaan dengan menganalisis regulasi nasional, dokumen Sistem Pemerintahan Berbasis Elektronik (SPBE), laporan Badan Siber dan Sandi Negara (BSSN), serta berbagai literatur ilmiah yang relevan. Hasil penelitian menunjukkan bahwa implementasi identitas digital di Kabupaten Barru masih berada pada tahap awal dengan tingkat interoperabilitas yang rendah, mekanisme autentikasi yang masih didominasi single-factor authentication, belum tersedianya Data Protection Officer (DPO), belum adanya regulasi daerah yang secara khusus mengatur perlindungan data, serta belum diterapkannya standar enkripsi secara menyeluruh. Kesenjangan tersebut menunjukkan bahwa tantangan implementasi tidak hanya bersifat teknis, tetapi juga berkaitan dengan kapasitas kelembagaan dan tata kelola. Penelitian ini merekomendasikan pembentukan regulasi daerah mengenai perlindungan data, penunjukan DPO, implementasi Multi-Factor Authentication (MFA), standardisasi enkripsi data, serta peningkatan literasi digital bagi aparatur pemerintah dan masyarakat guna mewujudkan tata kelola identitas digital yang aman, terintegrasi, dan berkelanjutan.

Kata Kunci: Identitas Digital; Sistem Pemerintahan Berbasis Elektronik (SPBE); Multi-Factor Authentication (MFA); Perlindungan Data Pribadi; Tata Kelola Digital.

ABSTRACT

Digital government transformation has positioned digital identity as a fundamental component of electronic public service delivery. However, the implementation of digital identity at the local government level continues to face significant challenges, particularly regarding authentication mechanisms, personal data protection, and institutional readiness. This study aims to analyze the implementation of digital identity in Barru Regency, evaluate the effectiveness of the existing authentication mechanisms, identify the gap between regulatory frameworks and actual data

protection practices, and formulate policy recommendations to strengthen digital identity governance. This research employed a descriptive qualitative approach through a literature study by examining national regulations, Electronic-Based Government System (SPBE) documents, National Cyber and Crypto Agency (BSSN) reports, and relevant scientific publications. The findings indicate that digital identity implementation in Barru Regency remains at an early stage, characterized by limited interoperability, reliance on single-factor authentication, the absence of a formally appointed Data Protection Officer (DPO), the lack of specific local regulations governing personal data protection, and the incomplete implementation of standardized data encryption. These findings suggest that the existing challenges are not merely technical but also institutional and governance-related. The study recommends establishing local regulations on data protection, appointing a DPO, implementing Multi-Factor Authentication (MFA), adopting standardized data encryption, and improving digital literacy among government officials and citizens to develop a secure, integrated, and sustainable digital identity governance framework.

Keywords: Digital Identity; Digital Government Services; Authentication Mechanism; Personal Data Protection; Multi-Factor Authentication (MFA).

A.PENDAHULUAN

Transformasi digital telah menjadi agenda strategis berbagai negara dalam meningkatkan kualitas tata kelola pemerintahan, efisiensi pelayanan publik, dan transparansi administrasi. Digitalisasi pemerintahan tidak lagi dipahami sekadar sebagai pemanfaatan teknologi informasi, tetapi sebagai proses transformasi kelembagaan yang mengintegrasikan teknologi, regulasi, tata kelola data, serta partisipasi masyarakat dalam penyelenggaraan layanan publik. Di Indonesia, percepatan transformasi digital diperkuat melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang mendorong seluruh instansi pemerintah untuk menyelenggarakan layanan berbasis elektronik secara terintegrasi. Keberhasilan implementasi SPBE sangat bergantung pada keberadaan sistem identitas digital yang mampu menjamin autentikasi pengguna, integritas data, interoperabilitas antarinstansi, serta perlindungan terhadap data pribadi warga negara. Tanpa sistem identitas digital yang aman dan terpercaya, digitalisasi layanan publik berpotensi menimbulkan berbagai risiko, seperti pencurian identitas, penyalahgunaan data pribadi, serangan siber, hingga menurunnya tingkat kepercayaan masyarakat terhadap pemerintah digital (Janowski, 2015; Organisation for Economic Co-operation and Development [OECD], 2020; Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018).

Identitas digital saat ini telah diakui sebagai fondasi utama dalam pembangunan ekosistem pemerintahan digital di berbagai negara. Bank Dunia menegaskan bahwa digital identity memungkinkan masyarakat memperoleh akses terhadap layanan publik, layanan keuangan, kesehatan, pendidikan, serta berbagai transaksi digital secara aman dan efisien sehingga berkontribusi terhadap peningkatan inklusi sosial dan ekonomi (World Bank, 2021). Demikian

pula International Telecommunication Union (ITU) menempatkan identitas digital sebagai komponen penting dalam membangun kepercayaan (digital trust) yang menjadi prasyarat keberhasilan transformasi digital nasional (International Telecommunication Union [ITU], 2023). Pengalaman Uni Eropa melalui penerapan Electronic Identification, Authentication and Trust Services (eIDAS) menunjukkan bahwa standardisasi identitas digital lintas negara mampu meningkatkan interoperabilitas layanan sekaligus memperkuat perlindungan data pribadi melalui mekanisme autentikasi yang berlapis dan tata kelola keamanan yang terstandarisasi (European Parliament & Council of the European Union, 2014). Keberhasilan tersebut memperlihatkan bahwa penguatan identitas digital tidak hanya memerlukan inovasi teknologi, tetapi juga dukungan regulasi, kelembagaan, serta koordinasi antarlembaga secara berkelanjutan.

Di Indonesia, pengembangan identitas digital terus mengalami perkembangan melalui implementasi Identitas Kependudukan Digital (IKD) yang dikelola oleh Kementerian Dalam Negeri sebagai bagian dari modernisasi administrasi kependudukan berbasis Nomor Induk Kependudukan (NIK). Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi semakin memperkuat landasan hukum pengelolaan identitas digital dengan menegaskan kewajiban setiap pengendali data untuk menjamin kerahasiaan, keamanan, dan akuntabilitas pengelolaan data pribadi. Meskipun demikian, berbagai laporan nasional masih menunjukkan bahwa implementasi keamanan sistem informasi pemerintah belum sepenuhnya memenuhi prinsip security by design maupun privacy by design. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa sebagian besar insiden keamanan siber pada instansi pemerintah masih dipicu oleh lemahnya mekanisme autentikasi, rendahnya penerapan enkripsi, serta minimnya kapasitas sumber daya manusia dalam pengelolaan keamanan informasi (Badan Siber dan Sandi Negara, 2023). Kondisi tersebut menunjukkan bahwa transformasi digital memerlukan penguatan aspek tata kelola keamanan siber agar manfaat digitalisasi tidak diikuti oleh meningkatnya risiko kebocoran data dan penyalahgunaan identitas digital.

Permasalahan tersebut menjadi semakin kompleks ketika dihadapkan pada kondisi pemerintah daerah yang memiliki tingkat kesiapan digital yang berbeda-beda. Kabupaten Barru merupakan salah satu daerah yang sedang berupaya mengimplementasikan berbagai kebijakan transformasi digital melalui penerapan SPBE, digitalisasi administrasi kependudukan, dan pengembangan layanan publik berbasis elektronik. Namun demikian, implementasi identitas digital di daerah masih menghadapi berbagai tantangan berupa keterbatasan interoperabilitas sistem, belum optimalnya penerapan Multi-Factor Authentication (MFA), belum tersedianya

regulasi teknis mengenai perlindungan data pribadi di tingkat daerah, serta terbatasnya jumlah sumber daya manusia yang memiliki kompetensi keamanan siber. Kesenjangan antara regulasi nasional dengan praktik implementasi di daerah menunjukkan bahwa keberhasilan transformasi digital tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh kapasitas kelembagaan, kepemimpinan digital, serta kesiapan organisasi dalam mengimplementasikan kebijakan secara konsisten (Nugroho, 2022; United Nations, 2024). Oleh karena itu, penelitian ini menjadi penting untuk menganalisis implementasi identitas digital di Kabupaten Barru, mengidentifikasi kesenjangan antara regulasi dan praktik perlindungan data, serta merumuskan rekomendasi kebijakan yang dapat memperkuat tata kelola identitas digital di tingkat pemerintah daerah.

Penelitian mengenai identitas digital, keamanan siber, dan perlindungan data pribadi dalam pemerintahan digital telah berkembang pesat dalam beberapa tahun terakhir. Ferdaus et al. (2022) menjelaskan bahwa keberhasilan implementasi identitas digital sangat dipengaruhi oleh integrasi antara teknologi, regulasi, dan kepercayaan pengguna. Penelitian lain menunjukkan bahwa autentikasi yang hanya mengandalkan kata sandi tidak lagi memadai untuk melindungi data pengguna dari ancaman phishing, credential stuffing, maupun serangan brute force yang semakin kompleks (Stallings, 2017). Di Indonesia, studi Pratama dan Sensuse (2021) menemukan bahwa sebagian besar pemerintah daerah masih berada pada tahap awal penerapan keamanan digital, ditandai dengan rendahnya adopsi Multi-Factor Authentication (MFA), belum optimalnya kebijakan keamanan informasi, serta minimnya pelatihan keamanan siber bagi aparatur pemerintah. Temuan tersebut menunjukkan bahwa keberhasilan implementasi identitas digital tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kapasitas organisasi dalam membangun budaya keamanan informasi yang berkelanjutan.

Meskipun berbagai penelitian telah membahas identitas digital dan perlindungan data pada sektor publik, masih terdapat kesenjangan penelitian yang perlu mendapat perhatian. Sebagian besar studi terdahulu berfokus pada aspek teknis keamanan sistem, evaluasi implementasi SPBE, atau analisis kebijakan perlindungan data pada level nasional. Penelitian yang secara khusus mengkaji keterkaitan antara implementasi identitas digital, efektivitas mekanisme autentikasi, dan kesenjangan regulasi perlindungan data pada konteks pemerintah daerah masih relatif terbatas, khususnya di wilayah Indonesia bagian timur. Padahal, karakteristik daerah yang memiliki keterbatasan infrastruktur digital, sumber daya manusia, dan kapasitas kelembagaan memerlukan pendekatan yang berbeda dibandingkan daerah perkotaan yang lebih maju secara teknologi. Menurut Heeks (2002), kegagalan transformasi digital di sektor publik sering kali disebabkan oleh

adanya kesenjangan antara desain kebijakan yang ideal dengan realitas organisasi yang menjalankannya. Perspektif tersebut menjadi relevan untuk memahami tantangan implementasi identitas digital pada pemerintah daerah seperti Kabupaten Barru.

Selain kesenjangan empiris, terdapat pula kebutuhan untuk memperkuat perspektif teoritis dalam kajian identitas digital di lingkungan pemerintahan daerah. Penelitian ini menggunakan pendekatan digital governance yang menempatkan teknologi, regulasi, sumber daya manusia, dan kepercayaan publik sebagai elemen utama keberhasilan transformasi digital (Janowski, 2015). Di samping itu, institutional theory digunakan untuk menjelaskan bagaimana tekanan regulatif dari pemerintah pusat mendorong pemerintah daerah mengadopsi sistem digital meskipun kapasitas kelembagaannya belum sepenuhnya siap (DiMaggio & Powell, 1983). Dalam banyak kasus, kondisi tersebut menghasilkan implementasi yang bersifat simbolik, yaitu sistem digital telah tersedia secara formal, tetapi belum didukung oleh tata kelola keamanan, perlindungan data, dan mekanisme pengawasan yang memadai. Oleh karena itu, penelitian ini tidak hanya mengidentifikasi kondisi implementasi identitas digital di Kabupaten Barru, tetapi juga menjelaskan faktor-faktor kelembagaan yang memengaruhi efektivitas penerapannya.

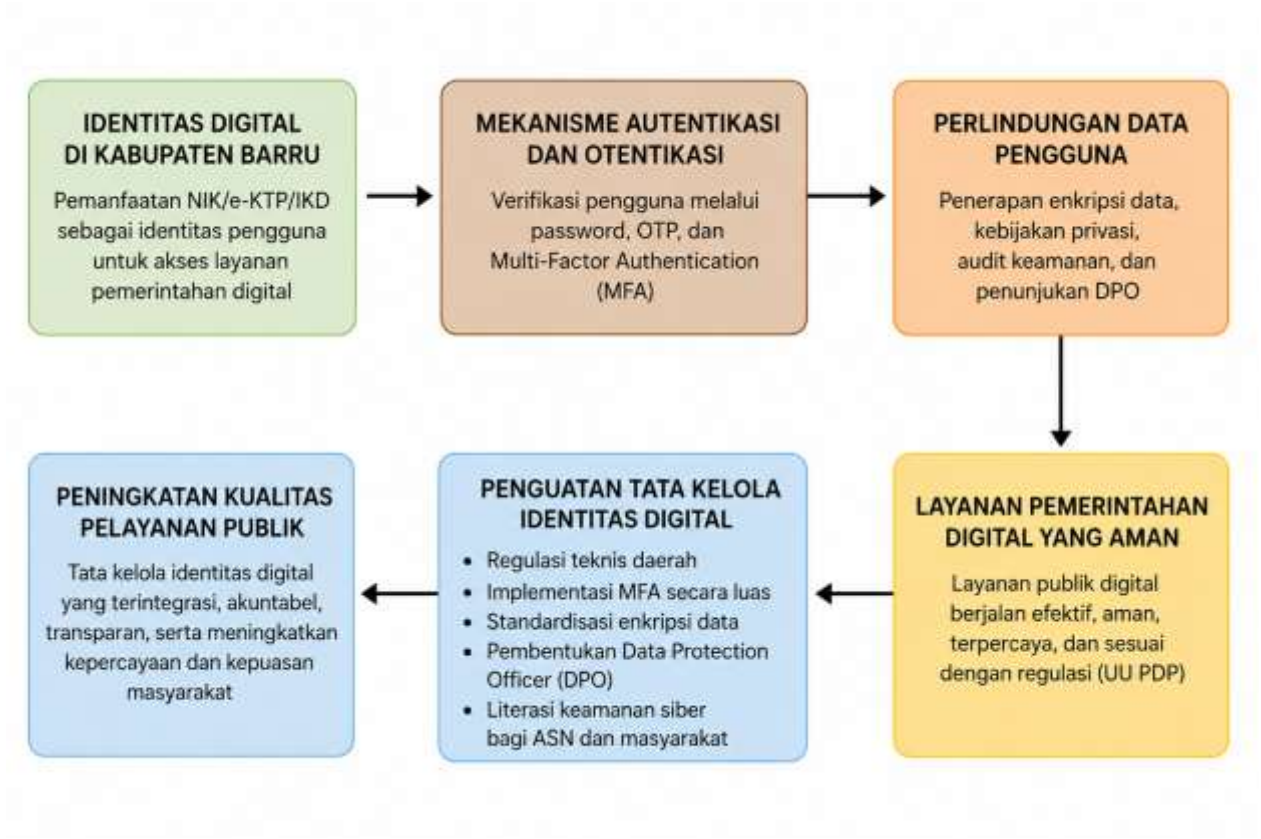
Berdasarkan uraian tersebut, penelitian ini menawarkan kebaruan (novelty) melalui analisis yang mengintegrasikan tiga dimensi utama, yaitu implementasi identitas digital, efektivitas mekanisme autentikasi, dan kesenjangan antara regulasi serta praktik perlindungan data pada tingkat pemerintah daerah. Berbeda dengan penelitian sebelumnya yang cenderung berfokus pada satu aspek tertentu, penelitian ini menghadirkan perspektif yang lebih komprehensif dengan mengaitkan aspek teknologi, kebijakan, dan tata kelola kelembagaan dalam satu kerangka analisis. Hasil penelitian diharapkan dapat memberikan kontribusi teoritis bagi pengembangan kajian digital governance dan keamanan informasi sektor publik, sekaligus memberikan kontribusi praktis berupa rekomendasi kebijakan bagi Pemerintah Kabupaten Barru dalam memperkuat perlindungan data pribadi dan keamanan identitas digital. Dengan demikian, penelitian ini menjadi relevan dalam mendukung percepatan transformasi digital pemerintahan yang aman, terpercaya, dan berkelanjutan sesuai dengan agenda reformasi birokrasi digital di Indonesia.

B.METODE PENELITIAN

Penelitian ini menggunakan pendekatan **kualitatif** dengan desain **studi kepustakaan (library research)** untuk menganalisis implementasi identitas digital dan perlindungan data pada penyelenggaraan pemerintahan digital di Kabupaten Barru. Pendekatan ini dipilih karena

memungkinkan peneliti melakukan kajian secara komprehensif terhadap berbagai regulasi, kebijakan, laporan resmi, serta literatur ilmiah yang berkaitan dengan identitas digital, mekanisme autentikasi, dan perlindungan data pribadi dalam konteks Sistem Pemerintahan Berbasis Elektronik (SPBE). Sumber data penelitian meliputi bahan hukum primer berupa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, Permendagri Nomor 57 Tahun 2021, serta dokumen evaluasi SPBE Kementerian PANRB. Selain itu, penelitian juga memanfaatkan bahan hukum sekunder berupa artikel ilmiah terindeks Scopus dan Sinta, laporan Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Digital, World Bank, International Telecommunication Union (ITU), serta berbagai referensi ilmiah lain yang diterbitkan pada periode 2020–2025. Pemilihan literatur dilakukan secara purposive dengan mempertimbangkan relevansi topik, kredibilitas sumber, serta kemutakhiran publikasi agar menghasilkan analisis yang valid dan komprehensif.

Analisis data dilakukan menggunakan analisis isi (content analysis**)** sebagaimana dikembangkan oleh Krippendorff (2019), yang bertujuan mengidentifikasi makna, pola, dan hubungan antar konsep dalam berbagai dokumen yang dianalisis. Tahapan analisis meliputi reduksi data melalui proses seleksi dan kategorisasi informasi berdasarkan empat fokus penelitian, yaitu implementasi identitas digital, efektivitas mekanisme autentikasi, kesenjangan antara regulasi dan praktik perlindungan data, serta rekomendasi kebijakan penguatan tata kelola identitas digital. Selanjutnya, data disajikan dalam bentuk narasi analitis yang didukung tabel komparatif untuk mempermudah interpretasi hasil penelitian. Tahap akhir dilakukan melalui penarikan kesimpulan dengan membandingkan temuan dari berbagai sumber menggunakan teknik triangulasi sumber sehingga diperoleh tingkat konsistensi dan validitas yang tinggi. Untuk memperkuat interpretasi, hasil analisis juga dikaji menggunakan perspektif Digital Governance Theory (Janowski, 2015) dan Institutional Theory (DiMaggio & Powell, 1983), sehingga mampu menjelaskan keterkaitan antara aspek regulasi, kelembagaan, kapasitas organisasi, dan implementasi kebijakan identitas digital pada pemerintah daerah.



Gambar 1 Kerangka Pikir Penelitian Implementasi Digital Identity dan Authentication Mechanism dalam Perlindungan Data Pengguna pada Pelayanan Pemerintahan Digital di Kabupaten Barru

C.HASIL PENELITIAN DAN PEMBAHASAN

- Hasil Penelitian

1) Implementasi Identitas Digital di Kabupaten Barru

Implementasi identitas digital di Kabupaten Barru menunjukkan bahwa transformasi digital pemerintahan telah mengalami perkembangan, namun belum mencapai tahap integrasi yang optimal. Berbagai layanan pemerintahan telah memanfaatkan teknologi digital, seperti penerapan Sistem Informasi Pemerintahan Daerah (SIPD), digitalisasi administrasi kependudukan yang terhubung dengan Direktorat Jenderal Kependudukan dan Pencatatan Sipil, serta penggunaan aplikasi berbasis web pada sejumlah Organisasi Perangkat Daerah (OPD). Meskipun demikian, implementasi tersebut masih bersifat sektoral sehingga setiap OPD mengelola sistem informasi secara terpisah tanpa didukung interoperabilitas data yang memadai. Kondisi ini menyebabkan

proses autentikasi, otorisasi pengguna, dan pencatatan aktivitas (audit trail) belum berjalan secara terintegrasi dalam satu ekosistem identitas digital. Akibatnya, efisiensi pelayanan publik belum sepenuhnya tercapai karena pengguna masih harus melakukan autentikasi berulang pada berbagai aplikasi pemerintah yang berbeda. Temuan ini menunjukkan bahwa digitalisasi layanan di Kabupaten Barru masih berada pada tahap digitalisasi proses administrasi dan belum berkembang menuju tata kelola identitas digital yang terpadu.

Tabel 1 Kerangka Regulasi Identitas Digital dan Relevansinya bagi Kabupaten Barru

Regulasi	Cakupan Utama	Relevansi terhadap Identitas Digital
UU No. 27 Tahun 2022 tentang PDP	Perlindungan data pribadi, hak subjek data, kewajiban pengendali data	Menjadi landasan hukum perlindungan data dalam sistem identitas digital
Perpres No. 95 Tahun 2018 tentang SPBE	Integrasi layanan pemerintahan berbasis elektronik	Menjadi kerangka implementasi identitas digital antarinstansi
Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia	Standarisasi dan interoperabilitas data pemerintah	Mendukung integrasi data kependudukan berbasis NIK
Permendagri No. 57 Tahun 2021	Pengelolaan administrasi kependudukan digital	Dasar penerapan Identitas Kependudukan Digital (IKD)
Perda Kabupaten Barru No. 3 Tahun 2020	Penyelenggaraan pemerintahan digital daerah	Landasan implementasi layanan digital di Kabupaten Barru

Sumber: Diolah dari berbagai regulasi nasional dan daerah, 2024.

Berdasarkan Tabel 1 dapat diketahui bahwa Kabupaten Barru sebenarnya telah memiliki landasan regulasi yang cukup komprehensif dalam mendukung implementasi identitas digital. Akan tetapi, hasil analisis menunjukkan bahwa keberadaan regulasi nasional belum sepenuhnya diikuti dengan kebijakan teknis di tingkat daerah. Belum adanya Peraturan Bupati yang secara khusus mengatur standar perlindungan data, mekanisme autentikasi, pengelolaan hak akses, serta tata kelola keamanan informasi menyebabkan implementasi identitas digital berjalan secara parsial pada masing-masing OPD. Akibatnya, setiap perangkat daerah masih menerapkan prosedur yang berbeda dalam mengelola identitas pengguna dan data masyarakat. Kondisi tersebut menunjukkan bahwa tantangan utama implementasi bukan lagi terletak pada kekurangan regulasi nasional, melainkan pada lemahnya operasionalisasi kebijakan di tingkat pemerintah daerah yang berimplikasi terhadap efektivitas penyelenggaraan layanan publik digital.

2) Analisis Efektivitas Mekanisme Autentikasi

Untuk memperoleh gambaran mengenai tingkat kesiapan identitas digital, penelitian ini membandingkan kondisi Kabupaten Barru dengan benchmark nasional pada beberapa indikator utama. Analisis menunjukkan bahwa meskipun pemanfaatan identitas digital berbasis Nomor Induk Kependudukan (NIK) telah diterapkan pada sejumlah layanan pemerintahan, implementasinya masih belum terintegrasi dengan seluruh sistem pelayanan publik. Selain itu, mekanisme autentikasi masih didominasi oleh penggunaan **single-factor authentication** berupa kombinasi nama pengguna dan kata sandi sehingga tingkat perlindungan terhadap akses tidak sah masih relatif rendah. Standar enkripsi data, kebijakan privasi, dan jumlah tenaga teknologi informasi yang memiliki kompetensi keamanan siber juga masih berada di bawah rata-rata pemerintah daerah yang telah menerapkan tata kelola digital secara lebih matang. Kondisi tersebut memperlihatkan bahwa kesiapan identitas digital di Kabupaten Barru masih memerlukan penguatan pada aspek teknologi, sumber daya manusia, serta tata kelola kelembagaan.

Tabel 2. Perbandingan Implementasi Identitas Digital Kabupaten Barru dengan Benchmark Nasional

Dimensi	Kabupaten Barru	Benchmark Nasional
Infrastruktur identitas digital	Sebagian terintegrasi	Terintegrasi pada sebagian besar layanan
Mekanisme autentikasi	Password tunggal	Multi-Factor Authentication (MFA)
Enkripsi data	Belum terstandarisasi	Mulai diterapkan secara luas
SDM keamanan siber	Terbatas	Lebih memadai
Regulasi teknis daerah	Belum tersedia	Sebagian daerah telah memiliki regulasi

Sumber: Analisis penulis berdasarkan data Kementerian PANRB, BSSN, dan Kementerian Komunikasi dan Digital, 2024.

Hasil analisis pada Tabel 2 memperlihatkan bahwa kesenjangan paling besar terdapat pada mekanisme autentikasi dan kesiapan regulasi teknis daerah. Mayoritas aplikasi layanan publik di Kabupaten Barru masih menggunakan autentikasi berbasis kata sandi tanpa didukung autentikasi berlapis seperti OTP, token keamanan, maupun biometrik. Model autentikasi tersebut relatif mudah diterapkan, tetapi memiliki tingkat kerentanan yang tinggi terhadap serangan brute force, phishing, dan credential stuffing. Selain itu, belum adanya standar keamanan yang seragam menyebabkan setiap OPD menerapkan kebijakan autentikasi sesuai kebutuhannya masing-masing. Temuan ini menunjukkan bahwa peningkatan keamanan identitas digital tidak cukup hanya dengan

menambah infrastruktur teknologi, tetapi juga membutuhkan harmonisasi regulasi, penguatan kapasitas SDM, dan implementasi standar keamanan informasi yang konsisten pada seluruh layanan digital pemerintah daerah.

3) Kesenjangan antara Regulasi dan Praktik Perlindungan Data

Perlindungan data pribadi merupakan komponen fundamental dalam implementasi identitas digital karena menentukan tingkat keamanan informasi yang dikelola oleh pemerintah daerah. Hasil analisis menunjukkan bahwa meskipun Kabupaten Barru telah memiliki landasan hukum yang mengacu pada Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP), implementasinya masih menghadapi berbagai kendala pada aspek teknis maupun kelembagaan. Sebagian besar sistem layanan publik belum menerapkan standar keamanan yang seragam sehingga mekanisme enkripsi data, autentikasi berlapis, kebijakan privasi, serta audit keamanan belum dilaksanakan secara konsisten. Kondisi tersebut menunjukkan adanya kesenjangan antara amanat regulasi dengan praktik penyelenggaraan layanan digital di tingkat daerah. Akibatnya, pengelolaan data kependudukan dan data pribadi masyarakat masih memiliki potensi kerentanan terhadap akses yang tidak sah maupun penyalahgunaan informasi. Temuan ini mengindikasikan bahwa keberhasilan implementasi identitas digital tidak hanya ditentukan oleh keberadaan regulasi nasional, tetapi juga oleh kesiapan organisasi dalam menerjemahkan regulasi tersebut ke dalam prosedur operasional yang terstandarisasi.

Tabel 3 Matriks Kesenjangan Regulasi dan Praktik Perlindungan Data di Kabupaten Barru

Aspek	Amanat Regulasi	Kondisi Aktual	Tingkat Kesenjangan
Enkripsi data	Wajib melindungi data sensitif	Belum seluruh sistem menggunakan enkripsi end-to-end	Tinggi
Multi-Factor Authentication (MFA)	Autentikasi berlapis untuk data sensitif	Mayoritas masih menggunakan password tunggal	Tinggi
Kebijakan privasi	Wajib tersedia dan dipublikasikan	Belum seluruh OPD memiliki kebijakan privasi	Sedang–Tinggi
Audit keamanan	Audit keamanan dilakukan secara berkala	Belum dilaksanakan secara rutin	Tinggi
Data Protection Officer (DPO)	Penunjukan DPO sesuai UU PDP	Belum terdapat penunjukan resmi	Tinggi

Sumber: Diolah dari UU No. 27 Tahun 2022, Perpres No. 95 Tahun 2018, dan hasil analisis penulis, 2024.

Berdasarkan Tabel 3 dapat diketahui bahwa hampir seluruh indikator perlindungan data menunjukkan tingkat kesenjangan yang tinggi. Kesenjangan terbesar terdapat pada belum diterapkannya Multi-Factor Authentication (MFA), belum adanya Data Protection Officer (DPO), serta belum terselenggaranya audit keamanan informasi secara berkala. Kondisi tersebut mengindikasikan bahwa tata kelola keamanan informasi di Kabupaten Barru masih berorientasi pada pemenuhan fungsi layanan digital, tetapi belum sepenuhnya mengintegrasikan prinsip perlindungan data pribadi sebagaimana diamanatkan oleh UU PDP. Selain itu, belum adanya standar enkripsi end to end menyebabkan data yang diproses dan ditransmisikan antarsistem berpotensi mengalami intersepsi apabila terjadi gangguan keamanan. Oleh karena itu, peningkatan kapasitas kelembagaan dan penyusunan kebijakan teknis daerah menjadi kebutuhan yang mendesak untuk memperkuat keamanan identitas digital pada seluruh layanan publik berbasis elektronik.

4) Analisis Teoretis dan Rekomendasi Kebijakan

Hasil penelitian menunjukkan bahwa permasalahan implementasi identitas digital di Kabupaten Barru tidak hanya dipengaruhi oleh keterbatasan teknologi, tetapi juga oleh faktor kelembagaan, regulasi, dan kapasitas sumber daya manusia. Dari perspektif **Digital Governance Theory**, keberhasilan transformasi digital bergantung pada keterpaduan antara teknologi, regulasi, organisasi, dan kepercayaan masyarakat. Temuan penelitian memperlihatkan bahwa keempat komponen tersebut belum berkembang secara seimbang sehingga implementasi identitas digital masih bersifat parsial. Di sisi lain, **Institutional Theory** menjelaskan bahwa pemerintah daerah cenderung mengadopsi kebijakan digital sebagai bentuk pemenuhan tuntutan regulasi nasional, namun perubahan pada praktik organisasi berlangsung lebih lambat akibat keterbatasan sumber daya dan belum tersedianya pedoman operasional yang rinci. Kondisi tersebut menyebabkan implementasi identitas digital lebih bersifat administratif daripada transformasional sehingga manfaat optimal dari digitalisasi layanan publik belum sepenuhnya dapat dirasakan oleh masyarakat.

Tabel 4 Prioritas Rekomendasi Penguatan Perlindungan Data Identitas Digital Kabupaten Barru

Prioritas	Rekomendasi	Aktor Utama	Target Waktu
P1	Pembentukan Tim Perlindungan Data dan penunjukan Data Protection Officer (DPO)	Bupati, Setda, Diskominfo	0–6 bulan
P1	Penyusunan Peraturan Bupati tentang Tata Kelola Identitas Digital	Bupati, DPRD, Bagian Hukum	0–12 bulan

P2	Implementasi Multi-Factor Authentication (MFA) pada seluruh layanan publik	Diskominfo, Vendor Sistem	6–18 bulan
P2	Standardisasi enkripsi data AES-256 pada seluruh sistem OPD	Diskominfo dan seluruh OPD	6–24 bulan
P3	Program literasi perlindungan data bagi ASN dan masyarakat	Diskominfo, Bappeda, Disdik	12–36 bulan

Sumber: Sintesis hasil analisis penelitian, 2024.

Berdasarkan Tabel 4, strategi penguatan perlindungan data di Kabupaten Barru perlu dilaksanakan secara bertahap sesuai tingkat urgensi dan kesiapan organisasi. Prioritas jangka pendek difokuskan pada pembentukan kelembagaan melalui penunjukan Data Protection Officer (DPO) dan penyusunan regulasi teknis sebagai dasar implementasi perlindungan data di lingkungan pemerintah daerah. Selanjutnya, prioritas jangka menengah diarahkan pada peningkatan keamanan sistem melalui penerapan Multi-Factor Authentication (MFA) dan standardisasi enkripsi data pada seluruh aplikasi layanan publik. Dalam jangka panjang, keberhasilan transformasi digital sangat ditentukan oleh peningkatan literasi digital aparatur dan masyarakat agar seluruh pemangku kepentingan memahami hak, kewajiban, serta risiko dalam pengelolaan data pribadi. Dengan implementasi kebijakan tersebut secara berkelanjutan, Kabupaten Barru berpotensi membangun ekosistem identitas digital yang lebih aman, terintegrasi, adaptif terhadap perkembangan teknologi, dan selaras dengan arah kebijakan transformasi digital nasional.

- Pembahasan

Hasil penelitian menunjukkan bahwa implementasi identitas digital di Kabupaten Barru masih berada pada tahap penguatan infrastruktur digital dan belum berkembang menjadi ekosistem identitas digital yang terintegrasi. Meskipun berbagai layanan pemerintahan telah memanfaatkan Sistem Informasi Pemerintahan Daerah (SIPD), aplikasi administrasi kependudukan, dan berbagai platform digital pada Organisasi Perangkat Daerah (OPD), integrasi data dan mekanisme autentikasi antar sistem belum berjalan secara optimal. Kondisi ini sejalan dengan teori Digital Governance yang dikemukakan Janowski (2015), yang menyatakan bahwa keberhasilan transformasi digital tidak hanya ditentukan oleh adopsi teknologi, tetapi juga oleh integrasi kelembagaan, interoperabilitas data, kapasitas sumber daya manusia, dan tata kelola yang efektif. Dengan demikian, digitalisasi layanan di Kabupaten Barru masih menunjukkan karakteristik digitalisasi administratif, yaitu memindahkan proses konvensional ke media elektronik tanpa didukung integrasi identitas digital secara menyeluruh. Temuan ini juga memperkuat laporan

OECD (2020) yang menyatakan bahwa interoperabilitas data merupakan faktor utama dalam meningkatkan efisiensi pelayanan publik dan kualitas pengambilan keputusan berbasis data.

Temuan penelitian juga mengungkap bahwa mekanisme autentikasi yang masih didominasi oleh **single-factor authentication** berupa penggunaan nama pengguna dan kata sandi menjadi salah satu kelemahan utama dalam perlindungan data pada layanan publik digital. Model autentikasi tersebut relatif mudah diterapkan, tetapi memiliki tingkat kerentanan yang tinggi terhadap berbagai bentuk serangan siber, seperti phishing, brute force, credential stuffing, maupun pengambilalihan akun. Hasil ini sejalan dengan laporan Badan Siber dan Sandi Negara (BSSN, 2023) yang menunjukkan bahwa sebagian besar insiden keamanan siber pada instansi pemerintah di Indonesia dipicu oleh lemahnya mekanisme autentikasi dan pengelolaan kredensial pengguna. Selain itu, penelitian Ferdaus et al. (2022) menegaskan bahwa implementasi **Multi-Factor Authentication (MFA)** mampu menurunkan risiko penyalahgunaan identitas digital secara signifikan karena mengombinasikan lebih dari satu faktor verifikasi. Oleh karena itu, penerapan MFA pada seluruh layanan publik di Kabupaten Barru menjadi kebutuhan strategis untuk meningkatkan keamanan sistem sekaligus memperkuat kepercayaan masyarakat terhadap layanan pemerintahan berbasis elektronik.

Penelitian ini juga menemukan adanya kesenjangan yang cukup besar antara regulasi nasional dan implementasi perlindungan data di tingkat pemerintah daerah. Meskipun Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi telah memberikan landasan hukum yang komprehensif, implementasinya di Kabupaten Barru belum didukung oleh regulasi teknis daerah, penunjukan **Data Protection Officer (DPO)**, audit keamanan informasi yang berkelanjutan, maupun penerapan standar enkripsi secara menyeluruh. Kondisi tersebut menunjukkan bahwa tantangan utama bukan lagi terletak pada aspek normatif, tetapi pada kapasitas kelembagaan dalam menerjemahkan regulasi ke dalam praktik administrasi pemerintahan. Temuan ini mendukung **Institutional Theory** yang dikemukakan DiMaggio dan Powell (1983), bahwa organisasi publik sering mengadopsi kebijakan baru sebagai respons terhadap tekanan regulatif, namun perubahan substantif dalam tata kelola berlangsung lebih lambat karena keterbatasan sumber daya, budaya organisasi, dan kesiapan kelembagaan. Oleh sebab itu, penguatan tata kelola perlindungan data perlu dilakukan secara sistematis melalui harmonisasi regulasi, penguatan organisasi, dan peningkatan kapasitas aparatur.

Berdasarkan keseluruhan hasil penelitian, penguatan identitas digital di Kabupaten Barru memerlukan pendekatan yang komprehensif dengan mengintegrasikan aspek regulasi, teknologi,

kelembagaan, dan pengembangan sumber daya manusia. Pembentukan regulasi teknis daerah mengenai perlindungan data, penunjukan Data Protection Officer (DPO), implementasi **Multi-Factor Authentication (MFA)**, standardisasi enkripsi data, serta peningkatan literasi keamanan siber bagi aparatur dan masyarakat merupakan langkah strategis untuk memperkuat keamanan layanan publik digital. Pendekatan tersebut sejalan dengan rekomendasi World Bank (2021) dan International Telecommunication Union (2023) yang menekankan bahwa keberhasilan implementasi identitas digital memerlukan keseimbangan antara inovasi teknologi, tata kelola kelembagaan, perlindungan hak privasi, dan peningkatan kepercayaan publik. Dengan demikian, transformasi digital di Kabupaten Barru tidak hanya diarahkan pada digitalisasi pelayanan, tetapi juga pada pembangunan ekosistem pemerintahan digital yang aman, akuntabel, berorientasi pada perlindungan data pribadi, serta mendukung terwujudnya tata kelola pemerintahan yang efektif, transparan, dan berkelanjutan.

D.KESIMPULAN DAN SARAN

- Kesimpulan

Penelitian ini menunjukkan bahwa implementasi identitas digital di Kabupaten Barru telah mendukung transformasi digital pemerintahan melalui pemanfaatan berbagai layanan berbasis elektronik, namun belum terintegrasi secara optimal dalam suatu ekosistem identitas digital yang aman dan terpadu. Hasil penelitian mengungkap bahwa tantangan utama terletak pada masih digunakannya mekanisme autentikasi berbasis single-factor authentication, belum tersedianya regulasi teknis daerah mengenai perlindungan data pribadi, belum adanya Data Protection Officer (DPO)**,** serta belum diterapkannya standar keamanan informasi seperti **Multi-Factor Authentication (MFA)** dan enkripsi data secara menyeluruh. Kesenjangan antara regulasi nasional dan implementasi di tingkat daerah menunjukkan bahwa keberhasilan transformasi digital tidak hanya bergantung pada ketersediaan teknologi dan kerangka hukum, tetapi juga pada kapasitas kelembagaan, kesiapan sumber daya manusia, serta komitmen pemerintah daerah dalam membangun tata kelola data yang akuntabel. Oleh karena itu, penguatan regulasi daerah, peningkatan keamanan sistem, pengembangan kompetensi aparatur, dan literasi perlindungan data menjadi langkah strategis untuk mewujudkan identitas digital yang aman, terpercaya, dan berkelanjutan dalam mendukung penyelenggaraan pemerintahan digital di Kabupaten Barru.

- Saran

Berdasarkan hasil penelitian, Pemerintah Kabupaten Barru disarankan untuk segera memperkuat tata kelola identitas digital melalui penyusunan regulasi teknis yang mengacu pada Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, termasuk pembentukan Data Protection Officer (DPO) sebagai penanggung jawab perlindungan data di lingkungan pemerintah daerah. Selain itu, implementasi **Multi-Factor Authentication (MFA)**, standardisasi enkripsi data, pelaksanaan audit keamanan informasi secara berkala, serta peningkatan interoperabilitas antar sistem informasi pemerintah perlu menjadi prioritas dalam pengembangan layanan publik digital. Penguatan kapasitas sumber daya manusia melalui pelatihan keamanan siber dan literasi perlindungan data bagi aparatur sipil negara maupun masyarakat juga perlu dilakukan secara berkelanjutan untuk meningkatkan kesadaran terhadap pentingnya keamanan informasi. Penelitian selanjutnya disarankan menggunakan pendekatan empiris melalui survei, wawancara, atau studi kasus pada berbagai pemerintah daerah sehingga dapat mengukur tingkat kematangan implementasi identitas digital serta menghasilkan model tata kelola yang lebih komprehensif dan dapat diadaptasi oleh daerah lain di Indonesia.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2023). *Laporan keamanan siber nasional 2023*. BSSN.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

European Parliament & Council of the European Union. (2014). *Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*. Official Journal of the European Union.

Ferdaus, M., Chowdhury, N., Alassafi, M. O., & Ali, M. (2022). Digital identity management systems for secure government services: A systematic literature review. *Government Information Quarterly, 39*(4), 101717. https://doi.org/10.1016/j.giq.2022.101717

Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The Information Society, 18*(2), 101–112. https://doi.org/10.1080/01972240290075039

International Telecommunication Union. (2023). *Global digital trends and trust framework report 2023*. ITU.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology* (4th ed.). Sage Publications.

Nugroho, Y. (2022). Implementasi sistem pemerintahan berbasis elektronik pada pemerintah daerah di Indonesia: Tantangan dan peluang transformasi digital. *Jurnal Administrasi Publik Indonesia, 8*(2), 145–160.

Organisation for Economic Co-operation and Development. (2020). *Digital government index: 2019 results*. OECD Publishing. https://doi.org/10.1787/4de9f5bb-en

Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Pratama, A. B., & Sensuse, D. I. (2021). Information security readiness in Indonesian local governments: Challenges toward digital government implementation. *Jurnal Sistem Informasi, 17*(1), 1–15.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

United Nations. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations.

World Bank. (2021). *ID4D global dataset 2021: Digital identification for development*. World Bank.