



**PERLINDUNGAN DATA PRIBADI DALAM IMPLEMENTASI DIGITAL  
IDENTITY DAN AUTHENTICATION MECHANISM PADA E-GOVERNMENT:  
ANALISIS BIBLIOMETRIK DAN KAJIAN KUALITATIF**

Sudirman

Program Studi Magister Administrasi Publik, ITBA Al Gazali Barru

[barrusudirman939@gmail.com](mailto:barrusudirman939@gmail.com)**ABSTRAK**

Penelitian ini bertujuan untuk menganalisis perkembangan penelitian mengenai perlindungan data pribadi dalam pemerintahan digital, mengidentifikasi tema-tema utama yang berkembang, serta menemukan peluang penelitian (*research gap*) terkait implementasi identitas digital dan mekanisme autentikasi dalam pelayanan publik. Penelitian menggunakan pendekatan kualitatif deskriptif dengan metode *Systematic Literature Review* (SLR) yang dipadukan dengan analisis bibliometrik menggunakan perangkat lunak VOSviewer. Data penelitian diperoleh dari artikel ilmiah nasional terakreditasi SINTA dan jurnal internasional bereputasi yang dikumpulkan melalui aplikasi *Publish or Perish*. Berdasarkan proses seleksi, diperoleh 22 artikel yang dianalisis menggunakan fitur *network visualization*, *overlay visualization*, dan *density visualization* pada VOSviewer. Hasil penelitian menunjukkan bahwa perkembangan kajian perlindungan data dalam pemerintahan digital membentuk tiga klaster utama, yaitu teknologi keamanan, regulasi perlindungan data, dan implementasi pelayanan publik berbasis digital. Analisis *overlay visualization* mengungkap bahwa penelitian mengenai integrasi Identitas Kependudukan Digital (IKD) dengan efektivitas pelayanan publik di tingkat daerah masih tergolong sebagai bidang penelitian yang berkembang (*emerging research area*). Selain itu, hasil penelitian menunjukkan bahwa implementasi identitas digital masih menghadapi berbagai tantangan, antara lain keterbatasan infrastruktur teknologi, lemahnya mekanisme autentikasi, rendahnya literasi digital, serta belum optimalnya implementasi regulasi perlindungan data pribadi. Penelitian ini memberikan kontribusi dalam mengidentifikasi arah pengembangan riset sekaligus menegaskan pentingnya integrasi aspek teknologi, regulasi, dan tata kelola pemerintahan untuk mewujudkan ekosistem pemerintahan digital yang aman, efektif, dan terpercaya.

**Kata Kunci:** identitas digital, perlindungan data pribadi, pemerintahan digital, VOSviewer, analisis bibliometrik.

**ABSTRACT**

This study aims to analyze the development of research on personal data protection in digital government, identify the major research themes, and explore research gaps related to digital identity implementation and authentication mechanisms in public services. The study employed a descriptive qualitative approach using a *Systematic Literature Review* (SLR) combined with bibliometric analysis using VOSviewer software. The data consisted of accredited national journal articles (SINTA) and reputable international publications collected through the *Publish or Perish* application. Following a systematic screening process, 22 articles were selected and analyzed

using VOSviewer through *network visualization*, *overlay visualization*, and *density visualization*. The findings reveal that research on data protection in digital government is organized into three major clusters: security technology, data protection regulation, and digital public service implementation. The *overlay visualization* indicates that studies integrating Digital Population Identity (Identitas Kependudukan Digital/IKD) with the effectiveness of local digital public services remain an emerging research area. Furthermore, the implementation of digital identity continues to face several challenges, including limited technological infrastructure, weak authentication mechanisms, low digital literacy, and suboptimal implementation of personal data protection regulations. This study contributes to identifying future research directions while emphasizing the importance of integrating technological, regulatory, and governance perspectives to establish a secure, reliable, and effective digital government ecosystem.

**Keywords:** digital identity, personal data protection, digital government, VOSviewer, bibliometric analysis.

## A.PENDAHULUAN



lisensi CC BY

Transformasi digital telah menjadi agenda strategis berbagai negara dalam meningkatkan efektivitas tata kelola pemerintahan dan kualitas pelayanan publik. Perkembangan teknologi informasi mendorong pemerintah untuk mengintegrasikan layanan publik ke dalam ekosistem digital yang lebih cepat, transparan, efisien, dan berorientasi pada kebutuhan masyarakat. Perserikatan Bangsa-Bangsa melalui *United Nations E-Government Survey 2024* menegaskan bahwa digital government tidak lagi dipahami sebatas digitalisasi layanan administrasi, tetapi sebagai model pemerintahan yang mampu mengintegrasikan data, teknologi, serta partisipasi masyarakat dalam mendukung pembangunan berkelanjutan (United Nations, 2024). Laporan tersebut menunjukkan bahwa perkembangan pemerintahan digital mengalami peningkatan di berbagai negara, meskipun masih terdapat kesenjangan kapasitas teknologi, infrastruktur, dan tata kelola antarnegara maupun antardaerah. Oleh karena itu, transformasi digital memerlukan dukungan kebijakan yang komprehensif, penguatan kelembagaan, serta sistem keamanan informasi yang mampu menjamin perlindungan hak-hak warga negara dalam memanfaatkan layanan digital (OECD, 2024; United Nations, 2024).

Indonesia turut menempatkan transformasi digital sebagai salah satu prioritas pembangunan nasional melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagaimana diatur dalam Peraturan Presiden Nomor 95 Tahun 2018. Kebijakan tersebut bertujuan meningkatkan kualitas tata kelola pemerintahan melalui integrasi sistem informasi, interoperabilitas data, dan penyelenggaraan pelayanan publik berbasis elektronik (Republik Indonesia, 2018). Sejalan dengan agenda tersebut, pemerintah mengembangkan Identitas

Kependudukan Digital (IKD) sebagai bentuk digitalisasi dokumen kependudukan yang memungkinkan masyarakat mengakses berbagai layanan publik secara lebih mudah melalui perangkat bergerak (*mobile device*). Implementasi IKD merupakan bagian dari strategi nasional untuk membangun identitas digital yang terintegrasi dengan berbagai layanan pemerintahan sekaligus mendukung terciptanya pelayanan publik yang lebih efisien, efektif, dan inklusif (Kementerian Dalam Negeri Republik Indonesia, 2022). OECD (2024) menjelaskan bahwa keberhasilan transformasi digital pemerintahan sangat dipengaruhi oleh kemampuan pemerintah dalam membangun sistem identitas digital yang terintegrasi, aman, dan berorientasi pada pengguna.

Keberadaan identitas digital merupakan komponen fundamental dalam penyelenggaraan pemerintahan digital karena berfungsi sebagai sarana autentikasi, verifikasi identitas, serta pengendalian akses terhadap berbagai layanan elektronik. Menurut World Bank melalui program *Identification for Development (ID4D)*, identitas digital yang aman menjadi prasyarat utama dalam memperluas akses masyarakat terhadap pelayanan publik, transaksi elektronik, perlindungan sosial, dan layanan keuangan digital (World Bank, 2024a). Identitas digital tidak hanya berfungsi sebagai alat verifikasi identitas, tetapi juga berperan dalam meningkatkan efisiensi administrasi pemerintahan serta memperkuat inklusi digital masyarakat. Di sisi lain, OECD (2024) menegaskan bahwa identitas digital harus dikembangkan berdasarkan prinsip keamanan, interoperabilitas, dan perlindungan hak privasi agar mampu meningkatkan kepercayaan masyarakat terhadap layanan pemerintah berbasis digital. Oleh karena itu, pembangunan sistem identitas digital harus dilakukan secara terpadu dengan penguatan tata kelola pemerintahan digital dan perlindungan data pribadi.

Meskipun memberikan berbagai manfaat, implementasi identitas digital juga menghadirkan tantangan yang semakin kompleks, khususnya terkait perlindungan data pribadi dan keamanan siber. Semakin besarnya volume data yang dikelola pemerintah meningkatkan risiko terjadinya penyalahgunaan informasi, pencurian identitas, maupun kebocoran data apabila sistem keamanan tidak dirancang secara memadai. Oleh karena itu, mekanisme autentikasi menjadi salah satu komponen utama dalam menjaga integritas dan kerahasiaan data masyarakat. Penggunaan teknologi seperti *multi-factor authentication (MFA)*, enkripsi data, dan autentikasi biometrik direkomendasikan sebagai standar keamanan dalam penyelenggaraan layanan pemerintahan digital (World Bank, 2024b). Dalam konteks Indonesia, implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi landasan hukum penting dalam memperkuat akuntabilitas pemerintah sebagai pengendali data sekaligus memberikan kepastian

hukum terhadap perlindungan hak privasi warga negara (Republik Indonesia, 2022). Namun demikian, efektivitas implementasinya masih memerlukan penguatan kapasitas kelembagaan, peningkatan infrastruktur digital, dan koordinasi antarinstansi agar transformasi digital dapat berlangsung secara aman, terpercaya, dan berkelanjutan (United Nations, 2024; OECD, 2024).

Perkembangan identitas digital juga membawa konsekuensi terhadap meningkatnya kebutuhan akan mekanisme autentikasi yang lebih kuat sebagai instrumen utama dalam menjamin keamanan sistem pemerintahan digital. Berbagai studi menunjukkan bahwa penggunaan autentikasi satu faktor (*single-factor authentication*) tidak lagi memadai dalam menghadapi kompleksitas ancaman siber yang terus berkembang. Oleh karena itu, banyak negara mulai menerapkan *Multi-Factor Authentication* (MFA), autentikasi biometrik, serta teknologi kriptografi untuk memperkuat keamanan akses terhadap layanan publik digital (OECD, 2024; World Bank, 2024a). Dalam konteks administrasi pemerintahan, mekanisme autentikasi yang andal tidak hanya berfungsi melindungi data pribadi masyarakat, tetapi juga menjaga integritas transaksi elektronik, mencegah penyalahgunaan identitas digital, serta meningkatkan kepercayaan masyarakat terhadap layanan pemerintah. Dengan demikian, keamanan autentikasi menjadi bagian yang tidak terpisahkan dari keberhasilan implementasi identitas digital dalam mewujudkan pelayanan publik yang efektif, transparan, dan akuntabel di era transformasi digital.

Di Indonesia, implementasi Identitas Kependudukan Digital (IKD) merupakan salah satu inovasi strategis pemerintah dalam mendukung percepatan transformasi digital pelayanan publik. Melalui Permendagri Nomor 72 Tahun 2022, pemerintah menetapkan standar penyelenggaraan IKD sebagai identitas resmi penduduk dalam bentuk digital yang dapat digunakan untuk mengakses berbagai layanan administrasi pemerintahan (Kementerian Dalam Negeri Republik Indonesia, 2022). Kehadiran IKD diharapkan mampu meningkatkan efisiensi pelayanan administrasi kependudukan, mengurangi penggunaan dokumen fisik, serta mendukung integrasi data kependudukan dalam ekosistem SPBE. Namun demikian, implementasi IKD masih menghadapi berbagai tantangan, seperti keterbatasan infrastruktur teknologi informasi, rendahnya literasi digital masyarakat, belum optimalnya interoperabilitas sistem antarinstansi, serta meningkatnya kekhawatiran masyarakat terhadap keamanan data pribadi. Kondisi tersebut menunjukkan bahwa keberhasilan implementasi identitas digital tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga oleh kesiapan regulasi, kelembagaan, dan kapasitas sumber daya manusia dalam mengelola layanan digital secara berkelanjutan (United Nations, 2024; World Bank, 2024b).

Seiring meningkatnya implementasi pemerintahan digital, penelitian mengenai identitas digital dan perlindungan data pribadi juga mengalami perkembangan yang cukup pesat. Namun demikian, hasil penelusuran literatur menunjukkan bahwa sebagian besar penelitian sebelumnya masih berfokus pada aspek keamanan siber, tata kelola teknologi informasi, maupun implementasi regulasi perlindungan data pribadi secara terpisah. Kajian yang mengintegrasikan hubungan antara identitas digital, mekanisme autentikasi, perlindungan data pribadi, dan efektivitas pelayanan publik berbasis digital masih relatif terbatas, khususnya dalam konteks pemerintahan daerah di Indonesia. Padahal, integrasi ketiga aspek tersebut sangat menentukan keberhasilan transformasi digital sektor publik karena menyangkut keamanan sistem, kepatuhan terhadap regulasi, serta kualitas pelayanan yang diterima masyarakat. Oleh sebab itu, diperlukan kajian yang mampu memetakan perkembangan penelitian sekaligus mengidentifikasi kecenderungan tema, hubungan antarkonsep, dan peluang penelitian yang masih terbuka sehingga dapat memberikan kontribusi terhadap pengembangan kebijakan pemerintahan digital di Indonesia (OECD, 2024; United Nations, 2024).

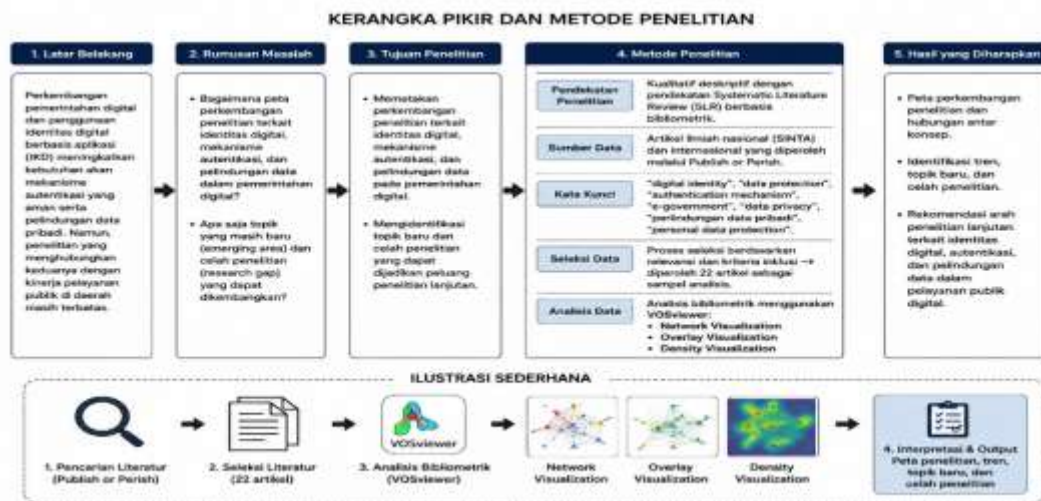
Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis perkembangan penelitian mengenai implementasi identitas digital, mekanisme autentikasi, dan perlindungan data pribadi dalam penyelenggaraan pemerintahan digital melalui pendekatan bibliometrik menggunakan perangkat lunak VOSviewer. Analisis dilakukan untuk memetakan hubungan antarkata kunci (*network visualization*), mengidentifikasi tren perkembangan penelitian (*overlay visualization*), serta menemukan kepadatan topik penelitian (*density visualization*) sehingga dapat diketahui arah perkembangan ilmu pengetahuan, *research gap*, dan *novelty* pada bidang kajian ini. Berbeda dengan penelitian sebelumnya yang lebih banyak menitikberatkan pada aspek teknologi atau regulasi secara parsial, penelitian ini menawarkan perspektif yang lebih komprehensif dengan menghubungkan dimensi keamanan autentikasi, perlindungan data pribadi, dan implementasi identitas digital dalam kerangka pemerintahan digital. Hasil penelitian diharapkan dapat memberikan kontribusi akademik terhadap pengembangan literatur serta menjadi masukan bagi pemerintah dalam memperkuat kebijakan transformasi digital yang aman, terpercaya, adaptif, dan berorientasi pada perlindungan hak-hak warga negara (World Bank, 2024a; OECD, 2024; United Nations, 2024)

## **B.METODE PENELITIAN**

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode *Systematic Literature Review* (SLR) yang dipadukan dengan analisis bibliometrik. Data penelitian diperoleh

dari artikel ilmiah nasional terakreditasi SINTA dan jurnal internasional bereputasi yang dikumpulkan melalui aplikasi *Publish or Perish* menggunakan kata kunci *digital identity*, *data protection*, *authentication mechanism*, *e-government*, *data privacy*, *perlindungan data pribadi*, dan *personal data protection*. Proses penelusuran literatur dilakukan secara sistematis melalui tahap identifikasi, penyaringan, dan seleksi berdasarkan relevansi topik penelitian sehingga diperoleh 22 artikel yang memenuhi kriteria inklusi dan dijadikan sebagai sampel penelitian. Seluruh referensi kemudian dikelola menggunakan aplikasi Zotero untuk memudahkan proses pengorganisasian dan pengelolaan data pustaka.

Analisis data dilakukan menggunakan perangkat lunak VOSviewer untuk memetakan perkembangan penelitian mengenai identitas digital dan perlindungan data dalam pemerintahan digital. Analisis bibliometrik meliputi *network visualization* untuk mengidentifikasi hubungan antarkata kunci, *overlay visualization* untuk menganalisis tren perkembangan penelitian dan menemukan *research gap* serta *novelty*, dan *density visualization* untuk mengetahui tingkat kepadatan serta dominasi topik penelitian dalam literatur yang dianalisis. Hasil visualisasi tersebut kemudian diinterpretasikan secara deskriptif guna menjelaskan perkembangan penelitian, keterkaitan antarkonsep, serta peluang pengembangan riset mengenai implementasi identitas digital, mekanisme autentikasi, dan perlindungan data pribadi dalam penyelenggaraan pemerintahan digital di Indonesia.



Gambar 1 Kerangka Pikir Metode Penelitian Analisis Bibliometrik Menggunakan VOSviewer

## C.HASIL PENELITIAN DAN PEMBAHASAN

### ➤ Hasil penelitian

Analisis Bibliometrik Perkembangan Riset (Data VOSviewer) Pengolahan data referensi yang mencakup 22 artikel utama menggunakan software VOSviewer menunjukkan gambaran mengenai perkembangan penelitian akademik mengenai perlindungan data pribadi, identitas digital, serta sistem autentikasi dalam konteks pemerintahan digital. Analisis bibliometrik dilakukan untuk mengetahui pola hubungan antar konsep, tema yang sering muncul, serta arah perkembangan penelitian yang ada dalam literatur ilmiah. Dengan menggunakan visualisasi jaringan, terlihat bahwa penelitian tentang keamanan data dan transformasi digital pemerintahan tidak hanya fokus pada satu sudut pandang, melainkan berkembang melalui beberapa pendekatan yang saling terkait, yaitu pendekatan teknologi, regulasi, dan penerapan layanan publik. Hasil pemetaan jaringan menunjukkan munculnya tiga klaster utama yang menjadi pusat perluasan penelitian. Klaster pertama berkaitan dengan aspek teknologi keamanan informasi serta cara mengenali identitas secara digital. Klaster ini terdiri dari istilah-istilah seperti mekanisme autentikasi, autentikasi multi-faktor (MFA), kriptografi, analisis biometrik, dan keamanan siber. Munculnya istilah-istilah tersebut menunjukkan bahwa kemajuan dalam pemerintahan digital sangat bergantung pada kemampuan sistem untuk memastikan bahwa setiap orang yang menggunakan layanan digital benar-benar memiliki identitas yang resmi dan sah. Dalam pelayanan publik yang berbasis digital, autentikasi tidak hanya sekadar hal teknis, tetapi juga menjadi dasar penting dalam membangun kepercayaan masyarakat terhadap layanan pemerintah.

Penggunaan autentikasi dengan dua faktor dan teknologi biometrik menjadi topik yang sering dibahas dalam penelitian karena semakin tingginya risiko ancaman terhadap keamanan data digital. Pemerintah yang memberikan layanan publik secara online perlu sistem pengenalan yang bisa memberi keseimbangan antara kemudahan dalam mengakses layanan dan tingkat keamanan yang baik. Sistem identitas digital seperti Identitas Kependudukan Digital (IKD) perlu dilindungi dengan beberapa lapisan keamanan agar data pribadi warga tidak dengan mudah dimanipulasi atau dipakai secara tidak sah. Oleh karena itu, banyak literatur dalam klaster ini menekankan betapa pentingnya menggabungkan teknologi enkripsi, proses autentikasi penggunaan. .

Klaster kedua menunjukkan perkembangan penelitian dari sudut pandang hukum, regulasi, serta perlindungan hak warga negara. Beberapa kata kunci yang paling banyak muncul

di klaster ini adalah data protection, privacy policy, personal data, UU PDP, dan constitutional rights. Ini menunjukkan pergeseran fokus penelitian, dari hanya membangun sistem digital menjadi bagaimana memastikan sistem tersebut berjalan sesuai dengan prinsip perlindungan hukum. Adanya peraturan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi hal yang penting yang mendorong perubahan cara pemerintah dalam mengelola data.

Dalam bidang pemerintahan, data warga adalah aset penting yang digunakan untuk berbagai hal, seperti urusan administrasi kependudukan, bantuan sosial, pembayaran pajak, dan pengembangan pembangunan. Namun, semakin tinggi ketergantungan pemerintah pada data digital, semakin tinggi pula kemungkinan adanya pelanggaran privasi jika pengelolaan data tidak dilakukan dengan baik. Oleh karena itu, penelitian ini menyoroti hubungan antara kewajiban pemerintah dalam menyediakan layanan digital dengan tanggung jawab pemerintah dalam memastikan keamanan dan kerahasiaan informasi warga masyarakat.

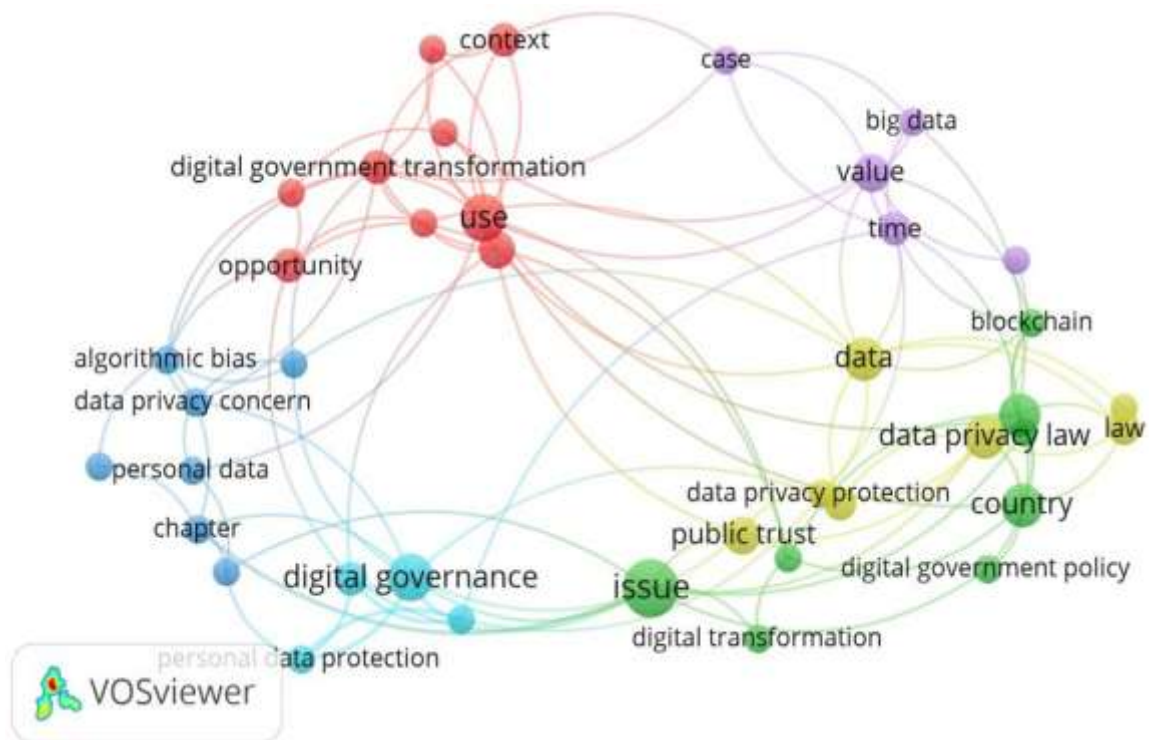
Berikutnya, klaster ketiga menggambarkan hal bagaimana pemerintahan digital diterapkan dalam bidang pelayanan publik. Istilah-istilah yang muncul dalam kelompok ini meliputi e-government, dompet digital identitas, penyediaan layanan publik, transformasi digital, dan reformasi birokrasi. Transformasi digital ini menunjukkan bahwa penggunaan teknologi tidak hanya tentang mengadopsi alat baru, tetapi juga tentang mengubah cara birokrasi bekerja dalam melayani masyarakat. Pemerintah diminta bukan hanya membuat aplikasi atau platform digital, tetapi juga memastikan teknologi tersebut bisa membuat pelayanan publik lebih efektif, efisien, transparan, dan berkualitas.

Berdasarkan hasil visualisasi overlay, perkembangan penelitian menunjukkan adanya beberapa bidang yang masih relatif baru (emerging research area). Penelitian yang langsung menghubungkan penggunaan identitas digital berbasis aplikasi seluler, seperti IKD, dengan kinerja pelayanan publik digital di daerah masih belum banyak dilakukan. Hal itu bisa dilihat dari letak beberapa kata kunci yang masih memiliki koneksi jaringan yang kurang kuat dan warna yang menunjukkan tingkat kemunculan penelitian yang masih tergolong baru. Kondisi itu menunjukkan bahwa masih ada celah dalam penelitian yang belum dijawab oleh literatur yang tersedia. Sebagian besar penelitian sebelumnya lebih fokus pada aspek teknis keamanan informasi atau aturan-aturan mengenai perlindungan data, tetapi belum banyak yang mempelajari bagaimana kedua hal tersebut bekerja sama dalam pelayanan administrasi pemerintahan. Padahal, kegagalan dalam proses autentikasi digital tidak hanya menyebabkan masalah teknis, tetapi juga bisa memengaruhi tanggung jawab pemerintah dalam memastikan

pelayanan yang aman dan dapat dipercaya.

Misalnya, ketika sistem autentikasi dalam layanan pemerintah digital mengalami kegagalan, masalah yang muncul tidak hanya terkait gangguan pada sistem tersebut, tetapi juga melibatkan siapa yang harus bertanggung jawab atas risiko kebocoran data warga, cara pemerintah mengembalikan layanan yang rusak, serta sejauh mana pemerintah telah menjalankan prinsip perlindungan data pribadi. Ini adalah hal yang penting bagi penelitian lanjutan. Dengan demikian, hasil analisis bibliometrik menggunakan VOSviewer menunjukkan bahwa penelitian tentang perlindungan data dalam pemerintahan digital berkembang melalui tiga aspek utama, yaitu teknologi keamanan, regulasi perlindungan data, dan penerapan layanan publik. Penelitian ini penting karena mencoba menghubungkan tiga aspek tersebut dengan meninjau keterkaitan antara mekanisme autentikasi digital, kepatuhan terhadap aturan perlindungan data pribadi, serta kualitas pelayanan publik yang berbasis digital. Pendekatan ini diharapkan bisa membantu dalam meningkatkan pengetahuan dan penerapan nyata untuk memperkuat pemerintahan digital yang aman, dapat dipercaya, dan menjaga hak-hak rakyat. Jaringan hubungan antarkonsep yang menjadi poros utama studi perlindungan data di sektor pemerintahan digital. Hasil visualisasi jaringan (*network visualization*) menunjukkan terbentuknya tiga klaster utama yang saling berkorelasi. Klaster pertama didominasi oleh term teknis operasional keamanan informasi seperti *authentication mechanism*, *multi-factor authentication (MFA)*, *cryptography*, dan *biometric analysis*. Klaster kedua berpusat pada dimensi hukum dan regulasi, yang ditandai oleh istilah *data protection*, *privacy policy*, *UU PDP*, dan *constitutional rights*. Sementara klaster ketiga mengarah pada dimensi implementasi sektoral seperti *e-government*, *digital identity wallets*, *public service delivery*, dan *bureaucratic reform*.

Peta perkembangan riset (*overlay visualization*) menyingkap fakta penting terkait kebaruan riset (*novelty*) dalam penelitian ini. Kajian mengenai integrasi identitas digital berbasis aplikasi seluler (seperti IKD) dan evaluasi efektivitas platform pelayanan publik digital di tingkat daerah (misalnya platform pajak online dan pencatatan sipil) berada pada klaster yang masih longgar dan berwarna pudar. Hal ini membuktikan bahwa riset yang menghubungkan secara langsung kegagalan teknis autentikasi dengan tanggung jawab administrasi negara pasca-berlakunya regulasi perlindungan data pribadi yang baru di Indonesia masih sangat terbatas. Penelitian ini hadir untuk mengisi celah riset tersebut dengan mengonfrontasikan teori hukum regulatif dengan kendala empiris yang dialami birokrasi.



**Gambar 2** Gambar graphic VOSviewer

Berdasarkan visualisasi Word Cloud yang dihasilkan melalui analisis frekuensi kata pada NVivo 12 Plus, istilah "digital", "birokrasi", "hukum", "kebijakan", dan "perlindungan" muncul sebagai konsep yang paling dominan diulas dalam literatur. Peneliti mengeksplorasi teks di balik kata kunci tersebut melalui tab Reference di NVivo untuk membedah permasalahan nyata dalam tata kelola e-government di Indonesia, yang kemudian diklasifikasikan ke dalam tiga tema besar:

1. Hambatan Substantif Implementasi Identitas Digital (Digital Identity)

Kajian kualitatif terhadap literatur menunjukkan bahwa peluncuran Identitas Kependudukan Digital (IKD) sebagai bagian dari penataan reformasi birokrasi digital masih membentur tembok kendala konstitusional dan hambatan teknis di tingkat daerah. Proses integrasi Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) ke dalam sistem pemerintahan berbasis elektronik (SPBE) sering kali tidak diiringi dengan kesiapan infrastruktur teknologi lokal yang memadai (Rahmawati et al., 2025). Kendala nyata yang ditemukan di lapangan mencakup ketidakstabilan server, rendahnya literasi digital masyarakat pengguna, hingga ketidakpastian hukum dalam hal koordinasi antar-instansi (Nurun, 2026). Akibatnya, masyarakat sering kali mengalami kegagalan sistem saat melakukan aktivasi atau sinkronisasi data pada aplikasi pelayanan publik daerah (Arieska, 2025).

2. Kerentanan Mekanisme Autentikasi (Authentication Mechanism) dan Celah Keamanan Ditinjau dari aspek keamanan informasi, permasalahan nyata yang paling krusial adalah mayoritas platform e-government di Indonesia masih mengandalkan mekanisme autentikasi faktor tunggal (*single-factor authentication*) yang sangat rentan terhadap serangan siber. Berdasarkan pelacakan referensi di NVivo, insiden kebocoran data pribadi di situs-situs pemerintah daerah dipicu oleh lemahnya manajemen kredensial akses dan ketiadaan enkripsi data yang terstandarisasi (Nurmansyah & Yustika, 2026). Kelemahan administratif ini mencakup kelalaian petugas pelaksana birokrasi dalam menjaga akun administrator internal sistem pelayanan (Islam & Sulastri, 2026). Tanpa adanya penerapan Multi-Factor Authentication (MFA) dan analisis penggunaan biometrik yang ketat, identitas digital warga negara yang tersimpan di dalam basis data nasional menjadi target yang sangat mudah bagi sindikat kejahatan siber internasional (Sitorus et al., 2025).

### 3. Dinamika Regulasi dan Tanggung Jawab Hukum Negara

Lahirnya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) seharusnya menjadi payung hukum tertinggi yang memaksa instansi pemerintah untuk memperketat sistem keamanannya. Namun, kajian kualitatif mendeteksi adanya fenomena "gagap regulasi" di mana banyak lembaga pemerintahan selaku pengelola data publik belum mampu memenuhi standar kepatuhan hukum yang diamanatkan undang-undang tersebut (Manurung, 2025). Terdapat ambiguitas nyata terkait bentuk pertanggungjawaban negara dan kejelasan fungsi otoritas pengawas independen ketika terjadi kebocoran data di platform e-government (Andriani & Haris, 2025). Akibatnya, penegakan sanksi administrasi terkesan tumpul jika pelanggaran dilakukan oleh sesama instansi pemerintah, yang pada akhirnya memperlemah pelindungan hak-hak warga negara di era digital (Abelia Mita Baqis & Muhammad Irwan Padli Nasution, 2025).

#### ➤ Pembahasan

Hasil analisis bibliometrik menggunakan VOSviewer menunjukkan bahwa kajian mengenai pelindungan data dalam pemerintahan digital berkembang melalui tiga dimensi utama, yaitu aspek teknologi keamanan, regulasi pelindungan data, dan implementasi pelayanan publik. Ketiga dimensi tersebut membentuk jaringan hubungan antarkonsep yang saling berkaitan dalam mendukung penyelenggaraan pemerintahan digital yang efektif dan aman. Klaster pertama menitikberatkan pada aspek teknis, seperti *authentication mechanism*, *multi-factor authentication* (MFA), *cryptography*, dan *biometric analysis*, yang berfungsi sebagai fondasi keamanan sistem digital. Klaster kedua menyoroti dimensi hukum melalui konsep *data*

*protection, privacy policy*, Undang-Undang Pelindungan Data Pribadi (UU PDP), dan *constitutional rights*, sedangkan klaster ketiga menekankan implementasi identitas digital dalam layanan pemerintahan, seperti *e-government, digital identity wallets, public service delivery*, dan *bureaucratic reform*. Temuan ini menunjukkan bahwa keberhasilan transformasi digital tidak hanya bergantung pada kemajuan teknologi, tetapi juga memerlukan harmonisasi antara aspek teknis, regulasi, dan tata kelola pelayanan publik. Dengan demikian, pelindungan data pribadi harus diposisikan sebagai bagian integral dari reformasi birokrasi digital untuk mewujudkan pelayanan publik yang aman, terpercaya, dan berorientasi pada kepentingan masyarakat.

Visualisasi *overlay* yang dihasilkan melalui VOSviewer juga mengungkap adanya peluang penelitian yang masih terbuka luas (*emerging research area*), khususnya mengenai implementasi identitas digital berbasis aplikasi seluler, seperti Identitas Kependudukan Digital (IKD), dalam meningkatkan efektivitas pelayanan publik di tingkat daerah. Warna yang relatif muda dan hubungan antarkata kunci yang masih longgar menunjukkan bahwa penelitian pada bidang tersebut masih terbatas dibandingkan dengan kajian mengenai keamanan informasi maupun regulasi pelindungan data. Sebagian besar penelitian terdahulu lebih banyak membahas aspek teknis autentikasi dan keamanan siber atau aspek normatif mengenai pelindungan data pribadi, sementara keterkaitan antara mekanisme autentikasi digital, kepatuhan terhadap regulasi, dan kualitas pelayanan publik masih belum banyak dieksplorasi. Padahal, keberhasilan implementasi identitas digital sangat ditentukan oleh kemampuan pemerintah dalam mengintegrasikan ketiga aspek tersebut secara simultan. Oleh karena itu, penelitian ini memberikan kontribusi kebaruan dengan menghubungkan dimensi teknologi, hukum, dan administrasi publik dalam satu kerangka analisis yang komprehensif sehingga dapat memperkaya literatur mengenai transformasi pemerintahan digital di Indonesia.

Temuan penelitian melalui analisis NVivo 12 Plus semakin memperjelas bahwa implementasi identitas digital di Indonesia masih menghadapi berbagai tantangan substantif. Hambatan tersebut meliputi keterbatasan infrastruktur teknologi informasi di daerah, rendahnya literasi digital masyarakat, belum optimalnya koordinasi antarinstansi, serta masih sering terjadinya gangguan sistem pada proses integrasi layanan publik. Di sisi lain, aspek keamanan informasi juga menjadi perhatian serius karena sebagian besar platform pemerintahan digital masih menggunakan mekanisme autentikasi faktor tunggal (*single-factor authentication*) yang memiliki tingkat kerentanan tinggi terhadap berbagai bentuk serangan siber. Kondisi tersebut meningkatkan risiko kebocoran data pribadi akibat lemahnya pengelolaan kredensial akses,

belum diterapkannya enkripsi yang memadai, serta minimnya implementasi teknologi *multi-factor authentication* (MFA) dan autentikasi biometrik. Temuan ini menunjukkan bahwa penguatan sistem keamanan digital tidak lagi menjadi pilihan, melainkan kebutuhan mendesak untuk menjamin keamanan identitas digital masyarakat sekaligus meningkatkan kepercayaan publik terhadap penyelenggaraan layanan pemerintahan berbasis elektronik.

Selain persoalan teknis, penelitian ini juga menunjukkan bahwa implementasi identitas digital masih menghadapi tantangan pada aspek regulasi dan pertanggungjawaban hukum negara. Meskipun Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi telah memberikan dasar hukum yang kuat bagi pengelolaan data pribadi, implementasinya di berbagai instansi pemerintah masih belum sepenuhnya optimal. Fenomena *regulatory gap* atau "gagap regulasi" terlihat dari belum seragamnya tingkat kepatuhan instansi pemerintah terhadap standar pelindungan data serta masih adanya ambiguitas mengenai mekanisme pertanggungjawaban ketika terjadi kebocoran data pada platform pemerintahan digital. Kondisi tersebut berpotensi melemahkan efektivitas penegakan hukum dan mengurangi kepercayaan masyarakat terhadap layanan digital pemerintah. Oleh karena itu, keberhasilan transformasi digital di Indonesia memerlukan penguatan tata kelola keamanan informasi, percepatan penerapan standar autentikasi yang lebih kuat seperti MFA dan biometrik, harmonisasi regulasi lintas sektor, serta peningkatan kapasitas kelembagaan dalam melaksanakan ketentuan UU Pelindungan Data Pribadi. Langkah-langkah tersebut diharapkan mampu mewujudkan ekosistem pemerintahan digital yang tidak hanya inovatif dan efisien, tetapi juga menjamin kepastian hukum, keamanan data, dan perlindungan hak-hak konstitusional warga negara.

#### **D.KESIMPULAN DAN SARAN**

##### ➤ Kesimpulan

Berdasarkan hasil analisis bibliometrik menggunakan VOSviewer dan analisis kualitatif melalui NVivo 12 Plus, dapat disimpulkan bahwa penelitian mengenai pelindungan data dalam pemerintahan digital berkembang melalui tiga dimensi utama, yaitu teknologi keamanan, regulasi pelindungan data, dan implementasi pelayanan publik berbasis digital. Hasil penelitian menunjukkan bahwa kajian yang menghubungkan identitas digital berbasis aplikasi seluler, seperti Identitas Kependudukan Digital (IKD), dengan efektivitas pelayanan publik di tingkat daerah masih relatif terbatas sehingga menjadi peluang penelitian yang memiliki nilai kebaruan. Selain itu, implementasi identitas digital di Indonesia masih menghadapi berbagai tantangan, antara lain keterbatasan infrastruktur teknologi, rendahnya literasi digital masyarakat, lemahnya

mekanisme autentikasi, serta belum optimalnya implementasi regulasi perlindungan data pribadi. Oleh karena itu, diperlukan penguatan tata kelola pemerintahan digital melalui penerapan mekanisme autentikasi yang lebih aman, harmonisasi regulasi, peningkatan kapasitas kelembagaan, serta penguatan perlindungan data pribadi agar transformasi digital mampu mewujudkan pelayanan publik yang efektif, aman, terpercaya, dan berorientasi pada perlindungan hak-hak warga negara.

#### ➤ Saran

Berdasarkan hasil penelitian, pemerintah perlu memperkuat implementasi identitas digital melalui pengembangan infrastruktur teknologi informasi yang lebih andal, terutama dengan menerapkan mekanisme keamanan yang lebih kuat seperti *Multi-Factor Authentication* (MFA), autentikasi biometrik, enkripsi data, serta sistem pemantauan keamanan siber secara berkelanjutan untuk meminimalkan risiko kebocoran data pribadi. Selain itu, diperlukan percepatan harmonisasi regulasi dan peningkatan koordinasi antarinstansi agar implementasi Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi dapat berjalan secara konsisten dalam seluruh layanan pemerintahan digital. Pemerintah juga perlu meningkatkan literasi digital aparatur dan masyarakat melalui program edukasi yang berkelanjutan sehingga penggunaan Identitas Kependudukan Digital (IKD) dapat diterima dan dimanfaatkan secara optimal. Bagi peneliti selanjutnya, disarankan untuk mengembangkan penelitian dengan mengkaji efektivitas implementasi identitas digital pada berbagai sektor pelayanan publik menggunakan pendekatan empiris, kuantitatif, atau *mixed methods*, sehingga dapat menghasilkan model tata kelola pemerintahan digital yang lebih komprehensif, aman, dan berorientasi pada perlindungan hak-hak warga negara.

### DAFTAR PUSTAKA

- Kementerian Dalam Negeri Republik Indonesia. (2022). *Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022 tentang Standar dan Spesifikasi Perangkat Keras, Perangkat Lunak, dan Blanko Kartu Tanda Penduduk Elektronik serta Penyelenggaraan Identitas Kependudukan Digital*. Kementerian Dalam Negeri. <https://peraturan.bpk.go.id/Home/Details/247019/permendagri-no-72-tahun-2022>
- OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*. OECD Publishing. <https://doi.org/10.1787/f64fed2a-en>

- OECD. (2024). *2023 OECD Digital Government Index: Results and key findings*. OECD Publishing. <https://doi.org/10.1787/1a89ed5e-en>
- OECD. (2024). *OECD Economic Surveys: Indonesia 2024*. OECD Publishing. <https://doi.org/10.1787/de87555a-en>
- Republik Indonesia. (2018). *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*. <https://peraturan.bpk.go.id/Home/Details/94599/perpres-no-95-tahun-2018>
- Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>
- United Nations. (2024). *United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development*. United Nations Department of Economic and Social Affairs. <https://desapublications.un.org/publications/un-e-government-survey-2024>
- World Bank. (2024a). *ID4D Annual Report 2024: Inclusive and trusted digital identity for development*. World Bank. <https://id4d.worldbank.org/>
- World Bank. (2024b). *Digital Progress and Trends Report 2024: Digital pathways for all*. World Bank. <https://www.worldbank.org/en/topic/digitaldevelopment>

**Peraturan PerUndang-Undangan**

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi