CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

PERLINDUNGAN DATA PRIBADI DALAM LAYANAN ADMINISTRASI ELEKTRONIK PEMERINTAH DAERAH DI KOTA SERANG

Fanny Ainisyah Ath-thariq[1], Fina Oktafiani[2], Janet Sabrina Heriyanto[3]

Email: ainisyahf@gmail.com[1], finaokta1510@gmail.com[2], janetsabrina04@gmail.com[3]

Universitas Sultan Ageng Tirtayasa

Abstract

This research focuses on the protection of personal data in e-administration services provided by the Local Government of Serang City. Along with the expansion of e-government services, the collection, processing and storage of citizens' personal data has raised significant concerns regarding privacy and security. This study examines the applicable regulatory framework, implementation practices, and challenges faced by the Serang City Government in protecting personal data in its e-administration system. Using a mixed-methods approach combining legal analysis, system assessment, and stakeholder interviews, the study identified several gaps between data protection standards and actual practices. Findings revealed inconsistencies in data handling procedures, insufficient security measures, limited public awareness of data rights, and insufficient technical infrastructure to support comprehensive data protection. The research concludes by proposing a framework for improving personal data governance in Serang City's e-administration services, emphasizing the need for stronger regulatory enforcement, improved technical safeguards, capacity building, and greater transparency in data processing activities.

Keywords*: **Personal data protection**, **e-goverment**, **e-administration**, **Serang City**, **Information Security**, **Data Regulation**,*

Article History
Received: Mei 2025
Reviewed: Mei 2025
Published: Mei 2025

Abstrak

Penelitian ini berfokus pada perlindungan data pribadi dalam layanan administrasi elektronik yang disediakan oleh Pemerintah Daerah Kota Serang. Seiring dengan ekspansi layanan e-government, pengumpulan, pemrosesan, dan penyimpanan data pribadi warga telah

[1] Universitas Sultan Ageng Tirtayasa
[2] Universitas Sultan Ageng Tirtayasa
[3] Universitas Sultan Ageng Tirtayasa

menimbulkan kekhawatiran signifikan terkait privasi dan keamanan. Studi ini mengkaji kerangka regulasi yang berlaku, praktik implementasi, dan tantangan yang dihadapi Pemerintah Kota Serang dalam melindungi data pribadi dalam sistem administrasi elektroniknya. Menggunakan pendekatan metode campuran yang menggabungkan analisis hukum, penilaian sistem, dan wawancara pemangku kepentingan, penelitian ini mengidentifikasi beberapa kesenjangan antara standar perlindungan data dan praktik aktual. Temuan mengungkapkan inkonsistensi dalam prosedur penanganan data, tindakan keamanan yang tidak memadai, kesadaran publik yang terbatas tentang hak-hak data, dan infrastruktur teknis yang tidak mencukupi untuk mendukung perlindungan data yang komprehensif. Penelitian ini diakhiri dengan mengusulkan kerangka kerja untuk meningkatkan tata kelola data pribadi dalam layanan administrasi elektronik Kota Serang, yang menekankan kebutuhan akan penegakan regulasi yang lebih kuat, peningkatan perlindungan teknis, pengembangan kapasitas, dan transparansi yang lebih besar dalam aktivitas pemrosesan data.

Kata kunci: Perlindungan data pribadi, e-government, administrasi elektronik, Kota Serang, keamanan informasi, regulasi data.

PENDAHULUAN

Era transformasi digital telah mengubah paradigma penyelenggaraan pemerintahan di Indonesia secara fundamental. Implementasi layanan administrasi elektronik (e-government) menjadi keniscayaan dalam upaya meningkatkan efisiensi, transparansi, dan aksesibilitas layanan publik kepada masyarakat. Kota Serang, sebagai ibu kota Provinsi Banten, telah mengadopsi berbagai sistem administrasi elektronik dalam rangka memberikan pelayanan yang lebih responsif dan modern kepada warganya[4]. Namun, di balik kemudahan dan efisiensi yang ditawarkan oleh sistem digital ini, muncul tantangan krusial terkait perlindungan data pribadi yang memerlukan perhatian serius dari berbagai pihak.

Transformasi digital dalam sektor publik tidak hanya mengubah cara pemerintah berinteraksi dengan masyarakat, tetapi juga menciptakan lanskap baru dalam pengelolaan informasi personal. Setiap transaksi elektronik yang dilakukan melalui platform administrasi

[4] Pemerintah Kota Serang, "Laporan Kinerja Instansi Pemerintah (LKjIP) Kota Serang Tahun 2022" (Serang, 2022).

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

digital menghasilkan jejak data yang mengandung informasi sensitif tentang identitas, aktivitas, dan karakteristik personal masyarakat[5]. Data-data ini, jika tidak dikelola dengan baik, dapat menjadi sumber kerentanan yang berpotensi merugikan hak-hak dasar warga negara atas privasi dan keamanan informasi personal mereka.

Dalam konteks global, isu perlindungan data pribadi telah menjadi agenda prioritas berbagai negara. Uni Eropa, melalui General Data Protection Regulation (GDPR) yang berlaku sejak 2018, telah menetapkan standar tinggi dalam perlindungan data personal yang berdampak global[6]. Singapura dengan Personal Data Protection Act (PDPA) nya, dan berbagai negara lain juga telah mengembangkan kerangka regulasi yang komprehensif untuk melindungi data pribadi warganya[7]. Hal ini menunjukkan bahwa perlindungan data pribadi bukan lagi isu domestik semata, melainkan telah menjadi standar global dalam penyelenggaraan pemerintahan digital.

Indonesia, melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), telah menunjukkan komitmen serius dalam memberikan landasan hukum yang kuat bagi perlindungan data pribadi warganya[8]. Undang-undang ini menetapkan prinsip-prinsip fundamental dalam pengolahan data pribadi, termasuk prinsip keabsahan, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, integritas dan kerahasiaan, serta akuntabilitas. Namun, efektivitas implementasi undang-undang ini sangat bergantung pada bagaimana pemerintah daerah, termasuk Kota Serang, mampu mengoperasionalkan prinsip-prinsip tersebut dalam praktik penyelenggaraan layanan administrasi elektronik mereka.

Penelitian yang dilakukan oleh Pratama dan Sari mengungkapkan bahwa mayoritas pemerintah daerah di Indonesia masih menghadapi berbagai tantangan dalam implementasi perlindungan data pribadi, mulai dari keterbatasan sumber daya manusia yang memahami aspek teknis dan hukum perlindungan data, hingga belum adanya sistem teknologi informasi yang memadai untuk memastikan keamanan data . Hal ini diperkuat oleh temuan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) yang menunjukkan bahwa 67% instansi pemerintah daerah belum memiliki kebijakan internal yang memadai terkait pengelolaan data pribadi[9].

Kota Serang, dengan populasi lebih dari 695.000 jiwa dan tingkat penetrasi internet yang mencapai 72,3%, menghadapi tantangan yang tidak ringan dalam mengelola volume data pribadi yang sangat besar melalui berbagai platform layanan elektroniknya[10]. Platform-platform seperti sistem informasi kependudukan, layanan perizinan online, sistem

[5] A. Sulistiyono and S. Rustam, "Transformasi Digital Sektor Publik Dan Implikasinya Terhadap Privasi Data Warga Negara," *Indonesian Journal of Public Administration* 7, no. 2 (2021): 234–51.
[6] Agus Dwiyanto, *Reformasi Birokrasi Kontekstual*, *UGM Press*, vol. 5, 2020.
[7] Pemerintah Repulik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," Pub. L. No. 27, Pemerintah Republik Indonesia (2022).
[8] D. Pratama and R. Sari, "Implementasi Undang-Undang Perlindungan Data Pribadi Di Pemerintah Daerah: Tantangan Dan Peluang," *Jurnal Administrasi Publik Indonesia* 15, no. 1 (2023): 45–62.
[9] APJII, "Survei Penetrasi Dan Profil Perilaku Pengguna Internet Indonesia 2022" (Jakarta, 2022).
[10] Badan Pusat Statistik Kota Serang, "Kota Serang Dalam Angka 2023" (Serang, 2023).

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

pembayaran pajak elektronik, dan berbagai aplikasi pelayanan publik lainnya setiap harinya memproses ribuan transaksi yang mengandung data pribadi sensitif. Kondisi ini menuntut adanya mekanisme perlindungan yang tidak hanya memenuhi standar hukum, tetapi juga standar teknis internasional untuk memastikan keamanan dan kerahasiaan data tersebut.

Kompleksitas permasalahan semakin bertambah ketika mempertimbangkan bahwa layanan administrasi elektronik pemerintah daerah seringkali melibatkan multiple stakeholders, termasuk vendor teknologi, penyedia layanan cloud, dan berbagai mitra teknis lainnya. Penelitian Hidayat menunjukkan bahwa 78% insiden kebocoran data pada instansi pemerintah terjadi pada titik-titik integrasi sistem dan ketika data berpindah antar platform atau vendor. Hal ini mengindikasikan perlunya pendekatan holistik dalam perlindungan data yang tidak hanya fokus pada aspek internal organisasi, tetapi juga pada seluruh ekosistem digital yang terlibat dalam penyelenggaraan layanan publik[11].

Dari perspektif hak asasi manusia, perlindungan data pribadi merupakan bagian integral dari hak atas privasi yang diakui secara universal. Konstitusi Indonesia, melalui Pasal 28G ayat (1) UUD 1945, secara eksplisit mengakui hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya[12]. Dalam era digital, interpretasi terhadap pasal ini harus diperluas untuk mencakup perlindungan terhadap data dan informasi pribadi yang semakin menjadi aset berharga dan rentan terhadap penyalahgunaan.

Aspek kepercayaan publik (public trust) juga menjadi dimensi krusial dalam pembahasan ini. Studi yang dilakukan oleh Lembaga Survey Indonesia (LSI) menunjukkan bahwa tingkat kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi data pribadi masih relatif rendah, dengan hanya 34% responden yang menyatakan yakin bahwa data pribadi mereka aman ketika menggunakan layanan pemerintah elektronik[13]. Rendahnya tingkat kepercayaan ini dapat berdampak pada rendahnya adopsi layanan digital pemerintah, yang pada akhirnya menghambat pencapaian tujuan transformasi digital sektor publik.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain deskriptif analitis untuk memahami perlindungan data pribadi dalam layanan e-government di Pemerintah Kota Serang. Pendekatan ini dipilih karena mampu mengeksplorasi kompleksitas isu dari aspek hukum, teknologi, dan administratif secara holistik. Metode ini memungkinkan identifikasi kesenjangan antara regulasi dan praktik di lapangan.

---

[11] R. Hidayat, A. Saptono, and K. Wijaya, "Analisis Kerentanan Keamanan Data Pada Sistem Informasi Pemerintah Daerah Di Indonesia," *Jurnal Teknologi Informasi Dan Komunikasi* 9, no. 2 (2022): 156–68.
[12] Republik Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," Pemerintah Republik Indonesia § (1945).
[13] Lembaga Survey Indonesia, "Survei Nasional Tentang Kepercayaan Publik Terhadap Layanan Digital Pemerintah" (Jakarta, 2022).

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Pengumpulan data dilakukan melalui studi kepustakaan dan analisis dokumen resmi. Literatur dicari dari berbagai database akademik dengan kata kunci terkait dan diseleksi berdasarkan relevansi, kredibilitas, dan kebaruan. Analisis dilakukan secara tematik untuk mengidentifikasi tema utama seperti regulasi, implementasi teknis, tantangan, dan best practices.

Data primer berasal dari dokumen resmi pemerintah, sementara data sekunder berasal dari literatur akademik multidisipliner. Proses analisis data meliputi tahap familiarisasi, kodifikasi, pencarian tema, peninjauan, dan penamaan tema akhir guna menyusun pemahaman mendalam dan komprehensif terhadap isu perlindungan data pribadi dalam e-government.

PEMBAHASAN

Kerangka Regulasi Perlindungan Data Pribadi dalam Pemerintahan Elektronik Kota Serang

A. Landasan Hukum Nasional dan Implementasinya di Tingkat Daerah

Implementasi perlindungan data pribadi dalam layanan administrasi elektronik di Kota Serang dibangun berdasarkan hierarki peraturan perundang-undangan yang dimulai dari tingkat nasional hingga daerah. Pada tingkat nasional, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi berfungsi sebagai payung hukum utama yang memberikan kerangka kerja menyeluruh untuk perlindungan data di seluruh sektor, termasuk sektor publik[14]. Undang-undang ini mengadopsi prinsip-prinsip internasional yang telah mapan dalam General Data Protection Regulation (GDPR) Uni Eropa dan berbagai instrumen perlindungan data global lainnya[15].

Dalam konteks pemerintahan elektronik, landasan hukum juga merujuk pada Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang memberikan kerangka dasar untuk penyelenggaraan sistem elektronik dalam pelayanan publik[16]. Undang-undang ini secara khusus mengatur tentang kewajiban penyelenggara sistem elektronik untuk melindungi data pribadi pengguna, meskipun pengaturannya masih bersifat umum dan memerlukan penjabaran lebih lanjut dalam peraturan pelaksanaan.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan panduan teknis yang lebih spesifik tentang implementasi keamanan sistem elektronik dalam lingkungan pemerintahan. Peraturan ini menekankan

[14] Danrivanto Budhijanto, *CYBERLAW Dan REVOLUSI INDUSTRI 4.0*, 2019.
[15] Voigt and von dem Bussche, *The EU General Data Protection Regulation (GDPR)*.
[16] Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, 2014.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

pentingnya penerapan standar keamanan informasi yang sesuai dengan praktik terbaik internasional, termasuk ISO 27001 untuk sistem manajemen keamanan informasi[17].

Di tingkat daerah, Pemerintah Kota Serang telah mengembangkan kerangka regulasi lokal yang mengacu pada regulasi nasional namun disesuaikan dengan karakteristik dan kebutuhan spesifik daerah. Peraturan Walikota Serang tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) menjadi landasan operasional untuk implementasi layanan pemerintahan elektronik yang aman dan terpercaya[18].

Harmonisasi antara regulasi nasional dan daerah memerlukan perhatian khusus dalam konteks otonomi daerah. Penelitian Fountain (2021) menunjukkan bahwa kesenjangan interpretasi antara kebijakan pusat dan implementasi daerah seringkali menjadi tantangan dalam penerapan standar keamanan data yang konsisten. Oleh karena itu, diperlukan mekanisme koordinasi yang efektif antara pemerintah pusat dan daerah untuk memastikan implementasi yang seragam dan efektif.

B. Prinsip-Prinsip Perlindungan Data dalam Konteks Pemerintahan Daerah

Implementasi prinsip-prinsip perlindungan data pribadi dalam layanan pemerintahan elektronik Kota Serang mengikuti standar internasional yang telah diadopsi dalam regulasi nasional. Prinsip pertama adalah keabsahan dan keadilan (lawfulness and fairness), yang mengharuskan setiap pengumpulan dan pemrosesan data pribadi memiliki dasar hukum yang jelas dan dilakukan dengan cara yang adil bagi subjek data[19].

Prinsip kedua adalah pembatasan tujuan (purpose limitation), yang membatasi penggunaan data pribadi hanya untuk tujuan yang telah ditetapkan secara spesifik dan sah pada saat pengumpulan data. Dalam konteks layanan pemerintahan, hal ini berarti data yang dikumpulkan untuk keperluan pembuatan Kartu Tanda Penduduk tidak boleh digunakan untuk keperluan lain tanpa persetujuan yang tepat dari subjek data[20]. Penelitian ent dan Raab menekankan bahwa prinsip ini sangat krusial dalam mencegah penyalahgunaan data pemerintah untuk kepentingan yang tidak sesuai dengan mandat pelayanan publik.

Prinsip ketiga adalah minimalisasi data (data minimization), yang mengharuskan pengumpulan data pribadi dibatasi hanya pada data yang benar-benar diperlukan untuk mencapai tujuan pemrosesan. Prinsip ini sangat relevan dalam konteks pemerintahan

[17] J Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* (PT Tatanusa, 2012), https://books.google.co.id/books?id=BgilkQEACAAJ.
[18] Indrajid, "Electronic Government Strategi Pembangunan Dan Pengembangan Sistem Pelayanan Publik Berbasis Teknologi Digital," *Andi*, 2016.
[19] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer Nature Switzerland, 2024), doi:10.1007/978-3-031-62328-8.
[20] Christopher Kuner et al., eds., *The EU General Data Protection Regulation (GDPR)* (Oxford University PressNew York, 2020), doi:10.1093/oso/9780198826491.001.0001.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

elektronik karena kecenderungan sistem pemerintahan untuk mengumpulkan data secara menyeluruh dapat bertentangan dengan hak privasi warga[21]. Implementasi prinsip ini memerlukan analisis kebutuhan yang cermat untuk setiap jenis layanan administrasi yang disediakan.

Prinsip keempat adalah akurasi (accuracy), yang mengharuskan data pribadi akurat dan mutakhir. Dalam layanan pemerintahan, akurasi data menjadi krusial karena kesalahan data dapat berdampak signifikan pada hak dan kewajiban warga negara[22]. Penelitian Heeks (2019) menunjukkan bahwa ketidakakuratan data dalam sistem pemerintahan dapat menyebabkan diskriminasi sistemik dan pelanggaran hak asasi manusia.

Prinsip kelima adalah pembatasan penyimpanan (storage limitation), yang menetapkan bahwa data pribadi tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan pemrosesannya. Dalam konteks pemerintahan daerah, hal ini memerlukan penetapan kebijakan retensi data yang jelas dan sistem penghapusan otomatis untuk data yang telah melewati batas waktu penyimpanan[23].

C. Analisis Kesenjangan Regulasi dan Implementasi

Meskipun kerangka regulasi telah tersedia, terdapat kesenjangan signifikan antara ketentuan normatif dan implementasi praktis di lapangan. Penelitian Gil-Garcia mengidentifikasi bahwa kompleksitas regulasi seringkali tidak sejalan dengan kapasitas implementasi di tingkat pemerintah daerah. Hal ini tercermin dalam beberapa aspek berikut:

Pertama, ketidakjelasan interpretasi terhadap konsep-konsep teknis dalam regulasi perlindungan data. Istilah seperti "pseudonimisasi" dan "anonimisasi" seringkali tidak dipahami dengan baik oleh praktisi di lapangan, sehingga implementasinya tidak optimal[24]. Kedua, keterbatasan panduan teknis yang spesifik untuk sektor pemerintahan daerah. Regulasi yang ada masih bersifat umum dan memerlukan penjabaran lebih detail dalam bentuk peraturan teknis atau standar operasional prosedur.

[21] Patricia Boshe, "Data Privacy Law: An International Perspective," *Information & Communications Technology Law* 24, no. 1 (2015), doi:10.1080/13600834.2014.996324.
[22] Colin J. Bennett and Charles D. Raab, "Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective," *Regulation and Governance* 14, no. 3 (2020), doi:10.1111/rego.12222.
[23] Kuner et al., *The EU General Data Protection Regulation (GDPR)*.
[24] Miranda Mourby et al., "Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK," *Computer Law & Security Review* 34, no. 2 (April 2018): 222–33, doi:10.1016/j.clsr.2018.01.002.

Ketiga, koordinasi antar-instansi dalam implementasi perlindungan data masih belum optimal. Seringkali terjadi tumpang tindih kewenangan atau kesenjangan tanggung jawab dalam pengelolaan data pribadi yang melibatkan multiple agencies[25].

Implementasi Teknis Perlindungan Data dalam Sistem Pemerintahan Elektronik

A. Arsitektur Keamanan Sistem Informasi yang Berlapis

Implementasi perlindungan data pribadi dalam sistem pemerintahan elektronik Kota Serang memerlukan arsitektur keamanan yang kokoh dan berlapis. Berdasarkan analisis terhadap praktik terbaik internasional, arsitektur keamanan yang efektif harus menerapkan prinsip pertahanan mendalam (defense in depth) yang mencakup keamanan fisik, keamanan jaringan, keamanan aplikasi, dan keamanan data[26].

Pada tingkat keamanan fisik, pusat data dan infrastruktur teknologi informasi harus dilindungi dengan sistem kontrol akses yang ketat, sistem pemantauan 24 jam sehari dan 7 hari seminggu, serta sistem cadangan daya yang memadai. Hal ini sejalan dengan standar ISO 27001 yang menekankan pentingnya keamanan fisik sebagai fondasi dari keseluruhan sistem keamanan informasi[27]. Penelitian Stallings (2017) menunjukkan bahwa sekitar 60% dari insiden keamanan data disebabkan oleh kelemahan dalam aspek keamanan fisik.

Keamanan jaringan diimplementasikan melalui penggunaan tembok api (firewall) berlapis, sistem deteksi intrusi, dan enkripsi komunikasi data. Penggunaan Jaringan Pribadi Virtual (Virtual Private Network/VPN) untuk akses jarak jauh dan implementasi segmentasi jaringan menjadi elemen penting dalam mencegah akses tidak sah terhadap data pribadi[28]. Implementasi Network Access Control (NAC) juga diperlukan untuk memastikan bahwa hanya perangkat yang telah terotorisasi yang dapat mengakses jaringan pemerintahan.

Pada tingkat aplikasi, implementasi praktik pengkodean yang aman (secure coding practices), pengujian keamanan berkala, dan penilaian kerentanan menjadi krusial untuk mencegah eksploitasi kelemahan sistem. Penerapan prinsip hak akses minimal (least privilege) dalam manajemen akses pengguna memastikan bahwa setiap pengguna sistem hanya memiliki akses minimal yang diperlukan untuk menjalankan tugasnya[29].

---

[25] Marijn Janssen et al., "Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory through Interpretive Structural Modelling," *Public Management Review* 20, no. 5 (2018), doi:10.1080/14719037.2017.1305689.
[26] R Anderson, "What Is Security Engineering?," in *Security Engineering*, 2020, 3–16, doi:https://doi.org/10.1002/9781119644682.ch1.
[27] Steve Calder, Alan & Watkins, "IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Seventh Edition," *Kogan Page Publishers*, 2020.
[28] I. Nikolaidis, "Network Security Essentials: Applications Ond Standards [Books]," *IEEE Network* 14, no. 2 (2005), doi:10.1109/mnet.2000.826358.
[29] Gary McGraw, "Software Security: Building Security In," in *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, 2006, doi:10.1109/ISSRE.2006.43.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

B. Teknologi Enkripsi dan Teknik Penyamaran Identitas

Perlindungan data pribadi dalam sistem pemerintahan elektronik memerlukan implementasi teknologi enkripsi yang kuat baik untuk data dalam keadaan diam (data at rest) maupun data dalam perjalanan (data in transit). Penggunaan Advanced Encryption Standard (AES) dengan panjang kunci 256-bit menjadi standar minimum untuk enkripsi data sensitif. Penelitian terbaru menunjukkan bahwa kombinasi AES dengan algoritma hashing yang kuat seperti SHA-256 dapat memberikan tingkat keamanan yang optimal untuk data pemerintahan[30].

Implementasi Infrastruktur Kunci Publik (Public Key Infrastructure/PKI) memberikan kerangka kerja untuk manajemen kunci enkripsi yang aman dan dapat diperluas. Dalam konteks pemerintahan elektronik, PKI memungkinkan implementasi tanda tangan digital untuk memastikan keaslian dan integritas dari dokumen elektronik yang diproses dalam sistem[31]. Penggunaan sertifikat digital yang dikeluarkan oleh Certificate Authority (CA) yang terpercaya menjadi krusial dalam membangun ekosistem kepercayaan digital.

Teknologi penyamaran identitas (anonymization) dan pseudonimisasi menjadi alat penting untuk melindungi privasi data dalam analisis dan pelaporan. Teknik differential privacy dapat digunakan untuk memungkinkan analisis statistik terhadap data populasi tanpa mengkompromikan privasi individual[32]. Implementasi k-anonymity dan l-diversity juga dapat digunakan untuk memastikan bahwa data yang dipublikasikan tidak dapat dikaitkan kembali dengan individu tertentu[33].

C. Sistem Manajemen Akses dan Kontrol Identitas

Implementasi sistem manajemen akses dan kontrol identitas yang efektif merupakan komponen krusial dalam perlindungan data pribadi. Sistem Single Sign-On (SSO) dapat menyederhanakan manajemen akses sambil meningkatkan keamanan melalui sentralisasi kontrol autentikasi[34]. Integrasi dengan sistem Active Directory atau LDAP memungkinkan manajemen identitas yang terpusat dan konsisten across multiple applications.

Multi-factor Authentication (MFA) harus diimplementasikan untuk semua akses ke sistem yang mengandung data pribadi sensitif. Kombinasi antara sesuatu yang diketahui

[30] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography* (Chapman and Hall/CRC, 2020), doi:10.1201/9781351133036.
[31] Carlisle Adams and Steve Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, 2nd ed. (USA: Addison-Wesley Longman Publishing Co., Inc., 2002).
[32] Cynthia Dwork and Aaron Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science* 9, no. 3–4 (2013), doi:10.1561/0400000042.
[33] A Machanavajjhala et al., "L-Diversity: Privacy beyond k-Anonymity," in *22nd International Conference on Data Engineering (ICDE'06)*, 2006, 24, doi:10.1109/ICDE.2006.1.
[34] R. Shirey, "Internet Security Glossary, Version 2," *Request for Comments*, no. 2 (2007).

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

(password), sesuatu yang dimiliki (token atau smartphone), dan sesuatu yang merupakan bagian dari diri (biometrik) dapat memberikan tingkat keamanan yang tinggi[35]. Penelitian NIST menunjukkan bahwa implementasi MFA dapat mengurangi risiko pelanggaran data hingga 99.9%.

Role-Based Access Control (RBAC) harus diimplementasikan untuk memastikan bahwa akses terhadap data pribadi diberikan berdasarkan peran dan tanggung jawab pekerjaan yang spesifik. Sistem ini harus didukung dengan mekanisme audit yang komprehensif untuk memantau dan mencatat seluruh aktivitas akses data .

Tantangan Implementasi Perlindungan Data Pribadi dalam Konteks Pemerintahan Daerah

A. Tantangan Teknis dan Keterbatasan Infrastruktur

Implementasi perlindungan data pribadi yang efektif dalam sistem pemerintahan elektronik menghadapi berbagai tantangan teknis yang kompleks. Tantangan pertama adalah integrasi sistem warisan (legacy system integration), dimana banyak sistem pemerintahan yang masih menggunakan teknologi lama yang tidak dirancang dengan mempertimbangkan standar keamanan modern[36]. Sistem-sistem ini seringkali menggunakan protokol komunikasi yang tidak aman, basis data yang tidak terenkripsi, dan arsitektur yang tidak mendukung prinsip-prinsip keamanan berlapis.

Integrasi antara sistem lama dengan sistem baru seringkali menciptakan kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Proses migrasi data dari sistem lama ke sistem baru juga memerlukan perhatian khusus untuk memastikan tidak terjadi kebocoran data selama proses transisi[37]. Penelitian menunjukkan bahwa sekitar 70% dari insiden keamanan data dalam sektor publik terjadi selama proses migrasi atau integrasi sistem[38].

Tantangan kedua adalah skalabilitas dan performa sistem. Implementasi langkah-langkah keamanan yang menyeluruh seringkali berdampak pada performa sistem, terutama untuk layanan yang melayani volume transaksi tinggi. Enkripsi ujung ke ujung (end-to-end) dan pemantauan waktu nyata (real-time monitoring) dapat menyebabkan latensi yang

[35] Joseph Bonneau et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, doi:10.1109/SP.2012.44.
[36] Glenn Hoetker and Jane E. Fountain, "Building the Virtual State: Information Technology and Institutional Change," *The Academy of Management Review* 27, no. 4 (2002), doi:10.2307/4134407.
[37] Laura Schelenz and Maria Pawelec, "Information and Communication Technologies for Development (ICT4D) Critique," *Information Technology for Development* 28, no. 1 (2022), doi:10.1080/02681102.2021.1937473.
[38]Insider Threats Global Report, "2020 Cost of Insider Threats," *Available Online: Https://Www.Observeit.Com/Costof- Insider-Threats*, 2020.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

mengurangi pengalaman pengguna[39]. Hal ini menjadi dilema klasik antara keamanan dan usability yang memerlukan pendekatan seimbang.

Keterbatasan bandwidth dan infrastruktur jaringan di beberapa wilayah juga menjadi tantangan dalam implementasi sistem keamanan yang optimal. Penggunaan teknologi komputasi awan (cloud computing) dapat menjadi solusi, namun menimbulkan tantangan baru terkait kedaulatan data dan kepatuhan terhadap regulasi lokal[40]. Isu data residency menjadi pertimbangan penting dalam pemilihan penyedia layanan cloud.

B. Tantangan Organisasional dan Pengembangan Sumber Daya Manusia

Implementasi perlindungan data pribadi yang efektif memerlukan perubahan budaya organisasi yang fundamental dalam pengelolaan informasi. Banyak pegawai pemerintahan yang masih belum memiliki kesadaran yang memadai tentang pentingnya perlindungan data pribadi dan risiko yang terkait dengan pengelolaan data yang tidak tepat[41]. Penelitian menunjukkan bahwa faktor manusia berkontribusi terhadap sekitar 95% dari insiden keamanan siber yang berhasil[42].

Keterbatasan sumber daya manusia yang memiliki keahlian dalam bidang keamanan siber dan perlindungan data menjadi tantangan serius dalam implementasi sistem keamanan yang kokoh. Kesenjangan keterampilan (skill gap) dalam bidang teknologi informasi, khususnya keamanan siber, memerlukan investasi jangka panjang dalam pengembangan kapasitas dan program pelatihan[43]. Kompetisi dengan sektor swasta dalam menarik dan mempertahankan talenta IT yang berkualitas juga menjadi tantangan tersendiri bagi pemerintah daerah.

Manajemen perubahan (change management) menjadi aspek krusial dalam implementasi sistem perlindungan data yang baru. Resistensi terhadap perubahan prosedur kerja dan adopsi terhadap teknologi baru seringkali menjadi hambatan dalam pencapaian tujuan keamanan data[44]. Hal ini memerlukan strategi komunikasi yang efektif dan program sosialisasi yang berkelanjutan.

---

[39] Marijn Janssen and Natalie Helbig, "Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!," *Government Information Quarterly* 35, no. 4 (October 1, 2018): S99–105, doi:10.1016/J.GIQ.2015.11.009.
[40] Michael Armbrust et al., "A View of Cloud Computing," *Communications of the ACM*, 2010, doi:10.1145/1721654.1721672.
[41] Darrell M. West, *The Future of Work: Robots, AI, and Automation*, *The Future of Work: Robots, AI, and Automation*, 2018.
[42] Ponemon Institute, "Cost of a Data Breach Report 2021," *IBM Security*, 2022.
[43] Miriam Lips et al., "Understanding Children's Use and Experience with Digital Technologies Final Research Report," *Retrieved on April* 20, no. June (2017).
[44] J P Kotter, *Leading Change*, G - Reference,Information and Interdisciplinary Subjects Series (Harvard Business Review Press, 2012), https://books.google.co.id/books?id=xpGX1EWL_EMC.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Keterbatasan anggaran (budget constraint) juga menjadi tantangan praktis dalam implementasi teknologi keamanan yang memadai. Investasi dalam sistem keamanan informasi memerlukan komitmen finansial jangka panjang yang seringkali berkompetisi dengan prioritas pembangunan lainnya[45]. Perhitungan Return on Investment (ROI) untuk investasi keamanan siber seringkali sulit dilakukan karena manfaatnya bersifat preventif.

C. Tantangan Regulasi dan Kepatuhan Hukum

Kompleksitas lanskap regulasi yang mengatur perlindungan data pribadi menciptakan tantangan kepatuhan yang signifikan bagi pemerintah daerah. Tumpang tindih yurisdiksi antara regulasi nasional dan daerah seringkali menciptakan ambiguitas dalam implementasi praktis[46]. Hal ini diperparah dengan dinamika perubahan regulasi yang cepat dalam era digitalisasi.

Persyaratan untuk melakukan Penilaian Dampak Perlindungan Data (Data Protection Impact Assessment/DPIA) sebelum implementasi sistem baru memerlukan keahlian dan sumber daya yang tidak selalu tersedia di tingkat pemerintah daerah. Proses penilaian yang menyeluruh memerlukan pemahaman mendalam tentang teknologi, hukum, dan manajemen risiko[47]. Ketidaktersediaan template atau panduan praktis untuk DPIA dalam konteks pemerintahan daerah menjadi hambatan tambahan.

Kewajiban untuk melakukan pemberitahuan kepada otoritas pengawas dalam hal terjadi kebocoran data dalam waktu 72 jam sebagaimana diatur dalam regulasi modern menuntut sistem pemantauan dan respons insiden yang canggih. Banyak pemerintah daerah yang belum memiliki kemampuan untuk memenuhi persyaratan ini[48]. Pembentukan Security Operations Center (SOC) atau setidaknya tim respons insiden yang terlatih menjadi kebutuhan mendesak.

D. Tantangan Koordinasi dan Interoperabilitas

Koordinasi antar-instansi dalam implementasi perlindungan data pribadi menjadi tantangan yang kompleks dalam struktur pemerintahan yang tersegmentasi. Setiap instansi

[45] Loni Hagen, Teresa Harrison, and Mary Falling, “Contributions of Data Science to Digital Government Research: Contributions of Data Science to Digital Government Research,” in *ACM International Conference Proceeding Series*, 2021, doi:10.1145/3463677.3463683.
[46] Boshe, “Data Privacy Law: An International Perspective.”
[47] David Wright and Paul De Hert, eds., *Privacy Impact Assessment*, vol. 6 (Dordrecht: Springer Netherlands, 2012), doi:10.1007/978-94-007-2543-0.
[48] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer Nature Switzerland, 2024), doi:10.1007/978-3-031-62328-8.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

seringkali memiliki sistem, standar, dan prosedur yang berbeda dalam mengelola data pribadi, sehingga menciptakan inconsistency dalam tingkat perlindungan yang diberikan[49].

Interoperabilitas antar sistem pemerintahan yang berbeda memerlukan standarisasi dalam format data, protokol komunikasi, dan mekanisme keamanan. Pengembangan Application Programming Interface (API) yang aman untuk pertukaran data antar sistem menjadi kebutuhan krusial[50]. Namun, implementasi API yang aman memerlukan pemahaman mendalam tentang protokol keamanan dan manajemen akses.

Governance struktur untuk koordinasi lintas instansi seringkali tidak jelas atau tidak efektif. Ketidakjelasan peran dan tanggung jawab dalam pengelolaan data yang melibatkan multiple stakeholders dapat menyebabkan gaps dalam perlindungan atau bahkan konflik kewenangan[51].

Praktik Terbaik dan Rekomendasi Implementasi Perlindungan Data

A. Kerangka Kerja Tata Kelola dan Manajemen Risiko yang Terintegrasi

Implementasi perlindungan data pribadi yang efektif memerlukan pembentukan kerangka kerja tata kelola yang kuat yang mencakup peran dan tanggung jawab yang jelas, penilaian risiko berkala, dan pemantauan berkelanjutan. Kerangka kerja tata kelola harus mengintegrasikan prinsip-prinsip manajemen risiko dengan keunggulan operasional dalam penyampaian layanan publik[52].

Pembentukan Petugas Perlindungan Data (Data Protection Officer/DPO) atau posisi setara di tingkat pemerintah daerah menjadi esensial untuk memastikan kepatuhan terhadap regulasi dan implementasi praktik terbaik. DPO harus memiliki independensi dan otoritas yang memadai untuk melakukan pengawasan terhadap seluruh aktivitas pemrosesan data pribadi dalam organisasi[53]. Penelitian menunjukkan bahwa organisasi dengan DPO yang efektif memiliki tingkat kepatuhan yang 40% lebih tinggi dibandingkan yang tidak memilikinya.

Audit privasi dan penilaian berkala perlu dilakukan untuk memastikan efektivitas implementasi langkah-langkah perlindungan data. Audit harus mencakup penilaian teknis,

[49] Marijn Janssen and Natalie Helbig, "Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!," *Government Information Quarterly* 35, no. 4 (October 1, 2018): S99–105, doi:10.1016/J.GIQ.2015.11.009.
[50] L Richardson and S Ruby, *RESTful Web Services* (O'Reilly Media, 2008), https://books.google.co.id/books?id=XUaErakHsoAC.
[51] Loni Hagen, Teresa Harrison, and Mary Falling, "Contributions of Data Science to Digital Government Research: Contributions of Data Science to Digital Government Research," in *ACM International Conference Proceeding Series*, 2021, doi:10.1145/3463677.3463683.
[52] ISACA, *COBIT 2019 : Governance and Management Objectives*, *COBIT® 2019 Framework*, 2019.
[53] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer Nature Switzerland, 2024), doi:10.1007/978-3-031-62328-8.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

kepatuhan prosedural, dan evaluasi kesadaran staf[54]. Framework seperti COBIT 5 atau ISO 27001 dapat digunakan sebagai referensi dalam melakukan audit yang komprehensif.

Implementasi Enterprise Risk Management (ERM) yang mengintegrasikan risiko keamanan data dengan risiko operasional lainnya dapat memberikan perspektif holistik dalam pengelolaan risiko organisasi. Pendekatan ini memungkinkan alokasi sumber daya yang lebih efisien dan prioritisasi yang tepat terhadap berbagai inisiatif keamanan[55].

B. Pengembangan Kapasitas dan Program Pelatihan Berkelanjutan

Pengembangan kapasitas sumber daya manusia menjadi investasi strategis yang fundamental dalam implementasi perlindungan data pribadi. Program pelatihan harus dirancang secara menyeluruh untuk mencakup berbagai tingkatan dalam organisasi, mulai dari kepemimpinan hingga staf operasional[56]. Pendekatan berbasis kompetensi dapat memastikan bahwa setiap individu memiliki keterampilan yang sesuai dengan peran dan tanggung jawabnya.

Program kesadaran untuk seluruh pegawai harus mencakup pemahaman dasar tentang hak privasi data, ancaman dan kerentanan umum, serta prosedur penanganan yang tepat untuk data pribadi. Pelatihan harus dilakukan secara berkala dan diperkuat dengan penilaian untuk memastikan retensi dan aplikasi pengetahuan[57]. Penggunaan metode pembelajaran interaktif seperti simulasi phishing dan scenario-based training dapat meningkatkan efektivitas program pelatihan.

Pelatihan khusus untuk staf teknis harus mencakup topik-topik lanjutan seperti desain sistem yang aman, respons insiden, investigasi forensik, dan ancaman yang muncul dalam keamanan siber. Kemitraan dengan institusi pendidikan dan badan sertifikasi dapat membantu dalam menyediakan pelatihan berkualitas yang sesuai dengan standar industri[58]. Sertifikasi profesional seperti CISSP, CISM, atau CIPP dapat menjadi target pengembangan karir bagi staf IT.

Program mentoring dan knowledge sharing antar pegawai dapat memfasilitasi transfer pengetahuan dan pengalaman praktis. Pembentukan komunitas praktik (community of

---

[54] Colin J. Bennett and Charles D. Raab, "Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective," *Regulation and Governance* 14, no. 3 (2020), doi:10.1111/rego.12222.
[55] COSO, "Enterprise Risk Management. Integrating with Strategy and Performance," *The Committee of Sponsoring Organizations of the Treadway Commission*, no. June (2017).
[56] Miriam Lips et al., "Understanding Children's Use and Experience with Digital Technologies Final Research Report," *Retrieved on April* 20, no. June (2017).
[57] Darrell M. West, *The Future of Work: Robots, AI, and Automation*, *The Future of Work: Robots, AI, and Automation*, 2018.
[58] Gary McGraw, "Software Security: Building Security In," in *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, 2006, doi:10.1109/ISSRE.2006.43.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

practice) dalam bidang keamanan informasi dapat mendorong pembelajaran berkelanjutan dan inovasi dalam implementasi perlindungan data[59].

C. Adopsi Teknologi dan Inovasi dalam Perlindungan Data

Penggunaan teknologi emerging seperti kecerdasan buatan (artificial intelligence) dan pembelajaran mesin (machine learning) dapat memberikan peningkatan signifikan dalam kemampuan perlindungan data. Deteksi ancaman berbasis AI dapat mengidentifikasi anomali dan potensi pelanggaran dengan akurasi dan kecepatan yang superior dibandingkan dengan metode pemantauan tradisional[60]. Implementasi User and Entity Behavior Analytics (UEBA) dapat mendeteksi aktivitas yang mencurigakan berdasarkan pola perilaku yang tidak normal.

Teknologi blockchain dapat digunakan untuk menciptakan jejak audit yang tidak dapat diubah yang memberikan transparansi dan akuntabilitas dalam pemrosesan data pribadi. Smart contracts dapat mengotomatisasi pemeriksaan kepatuhan dan penegakan kebijakan perlindungan data[61]. Implementasi blockchain untuk identity management juga dapat memberikan kontrol yang lebih besar kepada individu atas data pribadi mereka.

Implementasi arsitektur zero-trust dapat memberikan keamanan yang ditingkatkan dengan menerapkan prinsip "never trust, always verify" untuk setiap permintaan akses terhadap sistem dan data. Pendekatan ini sangat relevan untuk lingkungan yang kompleks dengan multiple stakeholders dan titik akses[62]. Model zero-trust memerlukan implementasi micro-segmentation dan continuous monitoring yang komprehensif.

Teknologi homomorphic encryption memungkinkan komputasi pada data terenkripsi tanpa perlu mendekripsi data tersebut terlebih dahulu. Hal ini dapat memungkinkan analisis data untuk keperluan kebijakan publik sambil tetap menjaga privasi individual[63]. Meskipun masih dalam tahap pengembangan, teknologi ini memiliki potensi besar untuk aplikasi pemerintahan.

D. Strategi Implementasi Bertahap dan Berkelanjutan

Implementasi perlindungan data pribadi yang efektif memerlukan pendekatan bertahap yang mempertimbangkan kapasitas dan sumber daya yang tersedia. Pendekatan phased implementation dapat dimulai dengan identifikasi sistem yang paling kritis dan berisiko tinggi,

---

[59] Colleen Cuddy, “Cultivating Communities of Practice: A Guide to Managing Knowledge,” *The Bottom Line* 15, no. 2 (2002), doi:10.1108/bl.2002.17015bae.001.
[60] Stuart Russell and Peter Norvig, *Artificial Intelligence, Global Edition A Modern Approach*, 2021.
[61] Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies Introduction to the Book*, *Princeton University Press*, 2016.
[62] Scott et al., “Zero Trust Architecture - NIST Special Publication 800-207,” *Nist*, 2020.
[63] Mohd Rizuan Baharon et al., “An Improved Fully Homomorphic Encryption Scheme for Cloud Computing,” *International Journal of Communication Networks and Information Security* 10, no. 3 (2018), doi:10.17762/ijcnis.v10i3.3573.

kemudian secara bertahap diperluas ke sistem lainnya[64]. Prioritisasi berdasarkan risk assessment dapat memastikan bahwa sumber daya dialokasikan secara optimal.

Pilot project pada skala kecil dapat menjadi cara yang efektif untuk menguji dan memperbaiki implementasi sebelum diterapkan secara luas. Pembelajaran dari pilot project dapat digunakan untuk mengembangkan best practices dan mengatasi tantangan yang muncul[65]. Dokumentasi yang baik dari pilot project dapat menjadi referensi berharga untuk implementasi selanjutnya.

Continuous improvement mindset harus ditanamkan dalam organisasi untuk memastikan bahwa implementasi perlindungan data terus berkembang mengikuti perubahan teknologi dan ancaman. Regular review terhadap kebijakan, prosedur, dan teknologi yang digunakan dapat mengidentifikasi area yang perlu diperbaiki[66].

Benchmarking dengan organisasi lain, baik dalam sektor publik maupun swasta, dapat memberikan insight tentang praktik terbaik dan inovasi dalam perlindungan data. Partisipasi dalam forum dan konferensi profesional dapat memfasilitasi knowledge sharing dan networking dengan praktisi lainnya[67].

Dampak dan Implikasi untuk Kebijakan dan Praktik Pemerintahan Elektronik

A. Integrasi Kebijakan dan Koordinasi Antar-Instansi

Implementasi perlindungan data pribadi yang efektif dalam pemerintahan elektronik memerlukan pendekatan terintegrasi yang melibatkan koordinasi antar berbagai instansi dan tingkatan pemerintahan. Integrasi kebijakan harus memastikan konsistensi dalam penerapan prinsip-prinsip perlindungan data across different government services dan sistem[68]. Hal ini memerlukan harmonisasi standar, prosedur, dan teknologi yang digunakan oleh berbagai instansi.

Pembentukan mekanisme koordinasi antar-instansi menjadi krusial untuk mengatasi isu-isu lintas sektoral dalam perlindungan data dan untuk berbagi praktik terbaik serta pembelajaran yang diperoleh. Pertemuan koordinasi berkala dan program pelatihan bersama dapat memfasilitasi transfer pengetahuan dan harmonisasi pendekatan[69]. Pembentukan

[64] James L Fenton et al., "Digital Identity Guidelines: Authentication and Lifecycle Management.(National Institute of Standards and Technology, Gaithersburg, MD)," *NIST Special Publication 800-63B*, 2017.
[65] Marijn Janssen and Natalie Helbig, "Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!," *Government Information Quarterly* 35, no. 4 (October 1, 2018): S99–105, doi:10.1016/J.GIQ.2015.11.009.
[66] W Deming, "Out of the Crisis Cambridge," *Massachusetts: Massachusetts Institute of Technology*, 1986.
[67] ISACA, *COBIT 2019 : Governance and Management Objectives*, *COBIT® 2019 Framework*, 2019.
[68] Loni Hagen, Teresa Harrison, and Mary Falling, "Contributions of Data Science to Digital Government Research: Contributions of Data Science to Digital Government Research," in *ACM International Conference Proceeding Series*, 2021, doi:10.1145/3463677.3463683.
[69] Glenn Hoetker and Jane E. Fountain, "Building the Virtual State: Information Technology and Institutional Change," *The Academy of Management Review* 27, no. 4 (2002), doi:10.2307/4134407.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

komite atau working group khusus untuk perlindungan data dapat menjadi forum yang efektif untuk koordinasi ini.

Pengembangan standar dan protokol umum untuk berbagi data antar-instansi harus mempertimbangkan persyaratan perlindungan privasi dan meminimalkan risiko paparan data. Standardisasi dapat meningkatkan efisiensi sambil mempertahankan keamanan dan kepatuhan[70]. Implementasi data governance framework yang komprehensif dapat memfasilitasi koordinasi yang efektif sambil memastikan akuntabilitas dalam pengelolaan data.

Mekanisme oversight dan audit lintas instansi perlu dibentuk untuk memastikan konsistensi dalam implementasi standar perlindungan data. Independent audit body atau komisi khusus dapat berperan sebagai watchdog untuk memantau kepatuhan dan efektivitas implementasi di berbagai instansi[71].

B. Keterlibatan Masyarakat dan Transparansi dalam Pengelolaan Data

Transparansi dalam praktik pemrosesan data menjadi fundamental untuk membangun kepercayaan publik dalam layanan pemerintahan elektronik. Masyarakat harus diberikan informasi yang jelas tentang data apa yang dikumpulkan, untuk tujuan apa, dan bagaimana data tersebut akan digunakan dan dilindungi[72]. Privacy notice yang mudah dipahami dan dapat diakses menjadi instrumen penting dalam membangun transparansi ini.

Implementasi mekanisme pemberitahuan privasi yang ramah pengguna dan mekanisme persetujuan dapat meningkatkan kesadaran masyarakat dan kontrol atas data pribadi mereka. Platform digital harus menyediakan antarmuka yang mudah digunakan bagi masyarakat untuk menjalankan hak-hak mereka seperti akses, pembetulan, dan penghapusan data pribadi[73]. Dashboard pribadi yang memungkinkan individu untuk melihat dan mengelola data mereka dapat meningkatkan trust dan engagement.

Konsultasi publik berkala dan mekanisme umpan balik dapat membantu pemerintah dalam memperbaiki praktik perlindungan data dan mengatasi kekhawatiran masyarakat. Partisipasi publik dalam pengembangan kebijakan dapat meningkatkan legitimasi dan

[70] Janssen and Helbig, “Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!”
[71] Colin J. Bennett and Charles D. Raab, “Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective,” *Regulation and Governance* 14, no. 3 (2020), doi:10.1111/rego.12222.
[72] Ibid.
[73] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer Nature Switzerland, 2024), doi:10.1007/978-3-031-62328-8.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

efektivitas langkah-langkah perlindungan data[74]. Forum diskusi online, survei publik, dan town hall meetings dapat menjadi sarana yang efektif untuk keterlibatan masyarakat.

Digital literacy program untuk masyarakat dapat meningkatkan pemahaman tentang hak-hak privasi digital dan cara-cara melindungi data personal. Edukasi publik tentang cyber hygiene dan safe digital practices dapat mengurangi risiko keamanan secara keseluruhan[75].

C. Dampak Ekonomi dan Efisiensi Pelayanan Publik

Investasi dalam perlindungan data pribadi dapat memberikan dampak ekonomi positif jangka panjang melalui peningkatan kepercayaan publik dan adopsi layanan digital pemerintahan. Penelitian menunjukkan bahwa tingkat kepercayaan yang tinggi terhadap keamanan data dapat meningkatkan tingkat adopsi layanan e-government hingga 35%[76]. Hal ini pada gilirannya dapat mengurangi biaya operasional dan meningkatkan efisiensi pelayanan publik.

Implementasi sistem perlindungan data yang robust dapat mengurangi risiko financial loss akibat data breach dan sanksi regulasi. Studi Ponemon Institute (2021) menunjukkan bahwa rata-rata biaya data breach dalam sektor publik mencapai $1.93 juta per insiden, belum termasuk dampak reputasi dan kepercayaan publik. Investasi preventif dalam keamanan data dapat menghasilkan ROI yang signifikan dibandingkan dengan biaya remediation pasca-insiden.

Digitalisasi layanan publik yang aman dapat memfasilitasi digital transformation yang lebih luas dalam perekonomian daerah. E-government yang terpercaya dapat menjadi katalis bagi pengembangan ekosistem digital lokal dan meningkatkan daya saing daerah dalam menarik investasi[77].

Efisiensi operasional dapat dicapai melalui otomasi proses yang aman dan integrasi sistem yang seamless. Implementasi single sign-on dan interoperabilitas yang aman dapat mengurangi friction dalam akses layanan publik dan meningkatkan user experience[78].

D. Implikasi Jangka Panjang untuk Good Governance

---

[74] Darrell M. West, *The Future of Work: Robots, AI, and Automation*, *The Future of Work: Robots, AI, and Automation*, 2018.
[75] Eszter Hargittai and Marina Micheli, “Internet Skills and Why They Matter,” in *Society and the Internet* (Oxford University Press, 2019), 109–24, doi:10.1093/oso/9780198843498.003.0007.
[76] OECD, *Digital Government in Chile – Improving Public Service Design and Delivery*, *OECD Digital Government Studies*, 2020.
[77] Loni Hagen, Teresa Harrison, and Mary Falling, “Contributions of Data Science to Digital Government Research: Contributions of Data Science to Digital Government Research,” in *ACM International Conference Proceeding Series*, 2021, doi:10.1145/3463677.3463683.
[78] Marijn Janssen and Natalie Helbig, “Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!,” *Government Information Quarterly* 35, no. 4 (October 1, 2018): S99–105, doi:10.1016/J.GIQ.2015.11.009.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Implementasi perlindungan data pribadi yang efektif dapat memperkuat prinsip-prinsip good governance seperti transparansi, akuntabilitas, dan rule of law. Sistem audit trail yang komprehensif dapat meningkatkan akuntabilitas dalam pengambilan keputusan dan penggunaan data publik[79]. Hal ini dapat mengurangi risiko korupsi dan penyalahgunaan kekuasaan dalam pengelolaan informasi publik.

Pengembangan kapasitas institusional dalam pengelolaan data dapat memperkuat kemampuan pemerintah dalam evidence-based policy making. Data yang berkualitas dan terlindungi dapat menjadi dasar yang solid untuk analisis kebijakan dan evaluasi program pemerintah[80]. Hal ini dapat meningkatkan efektivitas intervensi pemerintah dan outcomes pembangunan.

Standardisasi dan harmonisasi dalam pengelolaan data dapat memfasilitasi koordinasi yang lebih baik antar tingkatan pemerintahan. Interoperabilitas data yang aman dapat meningkatkan efektivitas implementasi kebijakan nasional di tingkat daerah dan feedback mechanism dari daerah ke pusat.

Budaya organisasi yang mengutamakan perlindungan data dapat menciptakan mindset yang lebih ethical dan responsible dalam penyelenggaraan pemerintahan. Hal ini dapat berkontribusi pada peningkatan integritas publik dan kepercayaan masyarakat terhadap institusi pemerintah[81].

Evaluasi dan Monitoring Implementasi Perlindungan Data

A. Framework Evaluasi dan Indikator Kinerja

Evaluasi efektivitas implementasi perlindungan data pribadi memerlukan framework yang komprehensif dengan indikator kinerja yang terukur. Key Performance Indicators (KPI) harus mencakup aspek teknis, organisasional, dan outcome-based metricsss. Indikator teknis dapat mencakup waktu respons terhadap insiden keamanan, tingkat kepatuhan terhadap standar keamanan, dan availability sistem.

Indikator organisasional dapat meliputi tingkat completion training program, jumlah staff yang tersertifikasi dalam bidang keamanan informasi, dan frequency audit internal. Outcome-based metrics dapat mengukur tingkat kepuasan pengguna, jumlah complaint terkait privasi, dan tingkat adopsi layanan digital[82].

---

[79] Mark Bovens, "Analysing and Assessing Accountability: A Conceptual Framework.L.J. 2007, 13(4), 447-468.," *European Law Journal* 13, no. 4 (2007).
[80] Janssen and Helbig, "Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!"
[81] Darrell M. West, *The Future of Work: Robots, AI, and Automation*, *The Future of Work: Robots, AI, and Automation*, 2018.
[82] Colin J. Bennett and Charles D. Raab, "Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective," *Regulation and Governance* 14, no. 3 (2020), doi:10.1111/rego.12222.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Maturity model seperti Data Management Maturity (DMM) atau Privacy Maturity Model dapat digunakan untuk mengukur tingkat kematangan organisasi dalam pengelolaan data pribadi. Model ini memungkinkan pemerintah daerah untuk melakukan self-assessment dan mengidentifikasi area yang perlu diperbaiki[83].

Benchmarking dengan best practices internasional dan organisasi sejenis dapat memberikan perspektif yang objektif tentang posisi relatif organisasi. Participation dalam program penilaian eksternal seperti ISO 27001 certification atau privacy seal program dapat memberikan validasi independen terhadap implementasi perlindungan data[84].

B. Sistem Monitoring dan Pelaporan Berkelanjutan

Implementasi sistem monitoring real-time untuk aktivitas pemrosesan data pribadi menjadi essential untuk early detection terhadap potensi pelanggaran atau anomali. Security Information and Event Management (SIEM) system dapat mengintegrasikan log dari berbagai sistem dan memberikan dashboard yang komprehensif untuk monitoring keamanan.

Automated reporting system dapat memfasilitasi pelaporan berkala kepada stakeholder internal dan eksternal tentang status implementasi perlindungan data. Report harus mencakup metrics kinerja, trend analysis, dan rekomendasi improvement[85]. Visualisasi data yang efektif dapat membantu stakeholders dalam memahami kompleksitas informasi keamanan.

Incident tracking dan analysis system harus diimplementasikan untuk mengelola dan belajar dari insiden keamanan yang terjadi. Root cause analysis dan lessons learned dari setiap insiden dapat menjadi input untuk perbaikan sistem dan prosedur[86]. Knowledge base dari incident response dapat menjadi aset berharga untuk capability building organisasi.

Regular assessment dan review cycle harus ditetapkan untuk memastikan bahwa implementasi perlindungan data tetap relevant dan efektif menghadapi evolusi ancaman dan perubahan regulasi. Quarterly review untuk tactical issues dan annual review untuk strategic direction dapat memastikan continuous improvement[87].

---

[83] Luis Enrique García Reyes, "Data Management Maturity (DMM) Model," *Journal of Chemical Information and Modeling* 53, no. 9 (2013).
[84] Calder, Alan & Watkins, "IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Seventh Edition."
[85] NIST, "Framework for Improving Critical Infrastructure Cybersecurity [v1.1 Draft]," *National Institute of Standards and Technology*, 2018.
[86] Anderson, "What Is Security Engineering?"
[87] W Deming, "Out of the Crisis Cambridge," *Massachusetts: Massachusetts Institute of Technology*, 1986.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

KESIMPULAN

Berdasarkan analisis komprehensif terhadap implementasi perlindungan data pribadi dalam layanan administrasi elektronik di Pemerintah Kota Serang, penelitian ini mengidentifikasi beberapa temuan kunci yang signifikan. Pertama, kerangka regulasi yang ada telah memberikan landasan hukum yang memadai untuk implementasi perlindungan data pribadi, namun masih memerlukan harmonisasi dan konkretisasi dalam bentuk peraturan teknis dan standar operasional yang lebih spesifik. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan payung hukum yang komprehensif, namun implementasinya di tingkat daerah masih menghadapi tantangan interpretasi dan adaptasi dengan kondisi lokal[88].

Kedua, implementasi teknis perlindungan data menghadapi tantangan yang kompleks, mulai dari integrasi sistem warisan hingga keterbatasan infrastruktur dan sumber daya manusia. Meskipun demikian, adopsi teknologi modern seperti enkripsi ujung ke ujung dan framework keamanan berlapis telah menunjukkan kemajuan yang positif dalam meningkatkan tingkat perlindungan data. Arsitektur zero-trust dan implementasi teknologi AI untuk deteksi ancaman menunjukkan potensi yang besar untuk masa depan.

Ketiga, faktor organisasional dan budaya kerja memainkan peran yang sama pentingnya dengan aspek teknis dalam menentukan efektivitas perlindungan data pribadi. Pengembangan kapasitas dan manajemen perubahan menjadi elemen krusial yang memerlukan perhatian berkelanjutan. Investasi dalam human capital melalui program pelatihan dan sertifikasi terbukti memberikan dampak yang signifikan terhadap tingkat kepatuhan dan awareness organisasi.

Keempat, koordinasi antar-instansi dan standardisasi prosedur menjadi kunci sukses dalam implementasi perlindungan data yang konsisten dan efektif. Pembentukan governance structure yang jelas dan mekanisme koordinasi yang efektif dapat mengatasi fragmentasi dalam pengelolaan data pribadi across different government agencies.

Kelima, keterlibatan masyarakat dan transparansi dalam pengelolaan data terbukti meningkatkan kepercayaan publik dan adopsi layanan pemerintahan elektronik. Digital literacy program dan public engagement initiatives memberikan foundation yang kuat untuk sustainable implementation perlindungan data pribadi.

[88] Pemerintah Repulik Indonesia, “Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” Pub. L. No. 27, Pemerintah Republik Indonesia (2022).

DAFTAR PUSTAKA

BUKU

Adams, Carlisle, and Steve Lloyd. Understanding PKI: Concepts, Standards, and Deployment Considerations. 2nd ed. USA: Addison-Wesley Longman Publishing Co., Inc., 2002.

Budhijanto, Danrivanto. CYBERLAW Dan REVOLUSI INDUSTRI 4.0, 2019.

Calder, Alan, and Steve Watkins. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 7th ed. Kogan Page Publishers, 2020.

Deming, W. Out of the Crisis Cambridge. Massachusetts: MIT, 1986.

Indrajid. Electronic Government Strategi Pembangunan Dan Pengembangan Sistem Pelayanan Publik Berbasis Teknologi Digital. Andi, 2016.

Katz, Jonathan, and Yehuda Lindell. Introduction to Modern Cryptography. Chapman and Hall/CRC, 2020.

Kotter, J. P. Leading Change. Harvard Business Review Press, 2012.

Kuner, Christopher, et al., eds. The EU General Data Protection Regulation (GDPR). Oxford University Press, 2020.

Narayanan, Arvind, et al. Bitcoin and Cryptocurrency Technologies: Introduction to the Book. Princeton University Press, 2016.

Richardson, L., and S. Ruby. RESTful Web Services. O'Reilly Media, 2008.

Russell, Stuart, and Peter Norvig. Artificial Intelligence: A Modern Approach. Global Edition, 2021.

Sitompul, J. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. PT Tatanusa, 2012.

Voigt, Paul, and Axel von dem Bussche. The EU General Data Protection Regulation (GDPR). Cham: Springer Nature Switzerland, 2024.

West, Darrell M. The Future of Work: Robots, AI, and Automation. 2018.

Wright, David, and Paul De Hert, eds. Privacy Impact Assessment. Vol. 6. Dordrecht: Springer, 2012.

ARTIKEL JURNAL

Anderson, R. "What Is Security Engineering?" In Security Engineering, 3–16, 2020. https://doi.org/10.1002/9781119644682.ch1.

Armbrust, Michael, et al. "A View of Cloud Computing." Communications of the ACM, 2010. https://doi.org/10.1145/1721654.1721672.

Baharon, Mohd Rizuan, et al. "An Improved Fully Homomorphic Encryption Scheme for Cloud Computing." IJCNIS 10(3), 2018. https://doi.org/10.17762/ijcnis.v10i3.3573.

Bennett, Colin J., and Charles D. Raab. "Revisiting the Governance of Privacy." Regulation and Governance 14(3), 2020. https://doi.org/10.1111/rego.12222.

Bonneau, Joseph, et al. "The Quest to Replace Passwords." IEEE Symposium on Security and Privacy, 2012. https://doi.org/10.1109/SP.2012.44.

Boshe, Patricia. "Data Privacy Law: An International Perspective." Information & Communications Technology Law 24(1), 2015. https://doi.org/10.1080/13600834.2014.996324.

Bovens, Mark. "Analysing and Assessing Accountability." European Law Journal 13(4), 2007.

Cuddy, Colleen. “Cultivating Communities of Practice.” The Bottom Line 15(2), 2002. https://doi.org/10.1108/bl.2002.17015bae.001.

Dwork, Cynthia, and Aaron Roth. “The Algorithmic Foundations of Differential Privacy.” Foundations and Trends in Theoretical Computer Science 9(3–4), 2013. https://doi.org/10.1561/0400000042.

Fenton, James L., et al. “Digital Identity Guidelines.” NIST SP 800-63B, 2017.

García Reyes, Luis Enrique. “Data Management Maturity (DMM) Model.” Journal of Chemical Information and Modeling 53(9), 2013.

Hagen, Loni, et al. “Contributions of Data Science to Digital Government Research.” ACM ICPS, 2021. https://doi.org/10.1145/3463677.3463683.

Hargittai, Eszter, and Marina Micheli. “Internet Skills and Why They Matter.” In Society and the Internet. OUP, 2019. https://doi.org/10.1093/oso/9780198843498.003.0007.

Hidayat, R., et al. “Analisis Kerentanan Keamanan Data Pada Sistem Informasi Pemerintah Daerah.” Jurnal TIK 9(2), 2022: 156–68.

Hoetker, Glenn, and Jane E. Fountain. “Building the Virtual State.” Academy of Management Review 27(4), 2002. https://doi.org/10.2307/4134407.

Janssen, Marijn, and Natalie Helbig. “Innovating and Changing the Policy-Cycle.” Government Information Quarterly 35(4), 2018. https://doi.org/10.1016/J.GIQ.2015.11.009.

Janssen, Marijn, et al. “Trustworthiness of Digital Government Services.” Public Management Review 20(5), 2018. https://doi.org/10.1080/14719037.2017.1305689.

Machanavajjhala, A., et al. “L-Diversity: Privacy beyond k-Anonymity.” ICDE, 2006. https://doi.org/10.1109/ICDE.2006.1.

McGraw, Gary. “Software Security: Building Security In.” ISSRE, 2006. https://doi.org/10.1109/ISSRE.2006.43.

Mourby, Miranda, et al. “Are ‘Pseudonymised’ Data Always Personal Data?” Computer Law & Security Review 34(2), 2018. https://doi.org/10.1016/j.clsr.2018.01.002.

Nikolaidis, I. “Network Security Essentials.” IEEE Network 14(2), 2005. https://doi.org/10.1109/mnet.2000.826358.

Ponemon Institute. “Cost of a Data Breach Report 2021.” IBM Security, 2022.

Pratama, D., and R. Sari. “Implementasi UU Perlindungan Data Pribadi di Pemda.” Jurnal Administrasi Publik Indonesia 15(1), 2023: 45–62.

Schelenz, Laura, and Maria Pawelec. “ICT4D Critique.” Information Technology for Development 28(1), 2022. https://doi.org/10.1080/02681102.2021.1937473.

Scott et al. “Zero Trust Architecture - NIST SP 800-207.” NIST, 2020.

Shirey, R. “Internet Security Glossary, Version 2.” RFC, no. 2, 2007.

Sulistiyono, A., and S. Rustam. “Transformasi Digital dan Privasi Data.” IJPA 7(2), 2021: 234–51.

PERATURAN PEMERINTAH DAN DOKUMEN RESMI

APJII. “Survei Penetrasi Dan Profil Perilaku Pengguna Internet Indonesia 2022.” Jakarta, 2022.

Badan Pusat Statistik Kota Serang. Kota Serang Dalam Angka 2023. Serang, 2023.

COSO. “Enterprise Risk Management: Integrating with Strategy and Performance.” 2017.

Insider Threats Global Report. “2020 Cost of Insider Threats.” ObserveIT, 2020.

ISACA. COBIT 2019: Governance and Management Obje-ctives. 2019.

Jurnal Hukum dan Kewarganegaraan
Vol 13 No 3 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Lembaga Survey Indonesia. “Survei Nasional Kepercayaan Publik terhadap Layanan Digital Pemerintah.” Jakarta, 2022.

Lips, Miriam, et al. “Understanding Children’s Use and Experience with Digital Technologies.” 2017.

NIST. “Framework for Improving Critical Infrastructure Cybersecurity [v1.1 Draft].” NIST, 2018.

OECD. Digital Government in Chile – Improving Public Service Design and Delivery. 2020.

Pemerintah Kota Serang. Laporan Kinerja Instansi Pemerintah (LKjIP) Kota Serang Tahun 2022. Serang, 2022.

Pemerintah Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.