E-ISSN: 3025-4698
P-ISSN: 3046-8582

Jurnal Pembangunan Kota Tangerang

Jurnal Pembangunan Kota Tangerang I Vol. 3 I No. 2 I Hal. 81 - 181 I Tahun 2025 I P-ISSN:3046-8582

Diterbitkan oleh:
Bappeda Kota Tangerang

PENGANTAR REDAKSI

Assalamu ‘alaikum wr. wb.

Puji syukur kita panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga Jurnal Pembangunan Kota Tangerang (JPKT) Volume 3 Nomor 2 ini dapat hadir ke hadapan para pembaca. Penerbitan edisi ini merupakan wujud komitmen kami untuk terus menyajikan gagasan-gagasan segar dan inovatif yang dapat mendorong percepatan pembangunan Kota Tangerang.. Edisi ini menghadirkan beragam gagasan, hasil pemikiran, serta inovasi yang berasal dari para peserta Lomba Karya Tulis Inovatif (LKTI) yang diselenggarakan oleh Badan Perencanaan Pembangunan Daerah (Bappeda) Kota Tangerang pada tanggal 2 September s.d. 3 November 2025.

Naskah-naskah yang tersaji dalam edisi ini merupakan representasi pemikiran kreatif dan solusi konstruktif dari berbagai kalangan, yang secara umum mencakup empat bidang strategis pembangunan daerah, yaitu: Ekonomi, Pemerintahan, Sosial, serta Sarana dan Prasarana. Setiap artikel membawa perspektif baru yang diharapkan dapat menjadi rujukan akademis sekaligus inspirasi dalam proses perencanaan dan pengambilan kebijakan pembangunan di Kota Tangerang.

Kami menyampaikan apresiasi setinggi-tingginya kepada seluruh peserta LKTI, tim penilai, mitra bestari, serta semua pihak yang telah berkontribusi dalam penyusunan dan penerbitan jurnal ini. Semoga hadirnya JPKT Volume 3 Nomor 2 dapat memberikan manfaat yang luas, memperkaya wacana pembangunan, serta mendorong tumbuhnya inovasi berkelanjutan di Kota Tangerang, serta sebagai upaya mendukung visi Kota Tangerang sebagai Kota yang Kolaboratif, Maju, Berkelanjutan, Sejahtera, dan Berakhlakul Karimah.

Akhir kata, kami berharap jurnal ini dapat menjadi salah satu media pengetahuan yang terus berkembang dan memberikan kontribusi nyata bagi masyarakat, akademisi, dan pemangku kepentingan pembangunan daerah.

Selamat membaca dan semoga bermanfaat.

Wassalamu ‘alaikum wr. wb.

KEPALA BAPPEDA KOTA TANGERANG

Dr. Hj. Yeti Rohaeti, AP., M.Si.
NIP. 19740807 199403 2 004

E-ISSN: 3025-4698
P-ISSN: 3046-8582

Jurnal Pembangunan
Kota Tangerang

Daftar Isi (Table of Content) Vol 3. No.2

Jurnal Pembangunan KotaTangerang
Vol. 3, No. 2, November 2025
P-ISSN 3046-8582 // E-ISSN 3025-4698

Kajian Keamanan Data Pengguna dalam Aplikasi Tangerang Live: Perspektif Regulasi dan Teknologi dalam Pemerintahan Digital

Data Security Study of User Information in the Tangerang Live Application: A Regulatory and Technological Perspective in Digital Governance

Rachmat Gustiana[1]

[1]Universitas Yuppentek Indonesia
Jl. Perintis Kemerdekaan I No.1, RT.007/RW.003, Babakan, Kec. Tangerang, Kota Tangerang, Banten 15118

Abstrak

Penelitian ini bertujuan untuk menganalisis keamanan data pengguna dalam aplikasi Tangerang Live, dengan fokus pada regulasi dan teknologi yang diterapkan dalam sistem pemerintahan digital. Pendekatan yang digunakan adalah kualitatif dengan studi kasus, yang mencakup wawancara mendalam, observasi, dan analisis dokumen terkait kebijakan perlindungan data pribadi. Hasil penelitian menunjukkan bahwa meskipun aplikasi Tangerang Live telah menerapkan enkripsi data dan autentikasi dua faktor (2FA), terdapat tantangan dalam pengelolaan server yang aman dan kurangnya pemahaman teknis di tingkat pengelola aplikasi mengenai regulasi perlindungan data pribadi. Aplikasi ini sudah mematuhi sebagian besar ketentuan dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), namun transparansi dalam pengelolaan data pribadi pengguna masih perlu ditingkatkan untuk memperkuat kepercayaan publik. Selain itu, penerapan teknologi blockchain dapat meningkatkan keamanan data dan transparansi, namun implementasinya terkendala oleh biaya dan kompleksitas. Penelitian ini merekomendasikan peningkatan infrastruktur keamanan, penggunaan teknologi canggih, edukasi literasi digital untuk pengguna, serta peningkatan transparansi dalam pengelolaan data. Penelitian ini diharapkan memberikan kontribusi dalam pengembangan kebijakan dan pengelolaan data dalam aplikasi pemerintahan digital di Indonesia.

Kata kunci: keamanan data, Tangerang Live, perlindungan data pribadi, teknologi blockchain, pemerintahan digital, transparansi

Abstract

This study aims to analyze the data security of users in the Tangerang Live application, focusing on the regulation and technology applied within the digital government system. A qualitative approach with a case study method was used, involving in-depth interviews, observations, and document analysis related to data privacy protection policies. The findings show that while Tangerang Live has implemented data encryption and two-factor authentication (2FA), challenges remain in secure server management and a lack of technical understanding among application administrators regarding data privacy regulations. The application complies with most provisions of the Personal Data Protection Law (UU PDP), but transparency in managing users' personal data still needs improvement to strengthen public trust. Additionally, the implementation of blockchain technology could enhance data security and transparency, although its adoption faces challenges due to cost and complexity. This study recommends enhancing security infrastructure, utilizing advanced technologies, digital literacy education for users, and improving transparency in data management. The research aims to contribute to policy development and data management practices in digital government applications in Indonesia.

Keywords: *data security, Tangerang Live, personal data protection, blockchain technology, digital government, transparency.*

Email:

[1]rgustiana08@gmail.com,

Cite This Article:

Gustiana, R (2025). Kajian Keamanan Data Pengguna dalam Aplikasi Tangerang Live : Perspektif Regulasi dan Teknologi dalam Pemerintahan Digital. Jurnal Pembangunan Kota Tangerang, 3(2), 108–116.

1. PENDAHULUAN

Perkembangan teknologi telah mentransformasi cara pemerintah berinteraksi dengan warganya, memunculkan era baru yang dikenal sebagai pemerintahan digital (e-government). Di tengah arus digitalisasi ini, Pemerintah Kota Tangerang mengambil langkah progresif dengan meluncurkan aplikasi Tangerang Live. Aplikasi ini bukan sekadar alat, melainkan sebuah ekosistem digital yang dirancang untuk mengintegrasikan berbagai layanan publik, mulai dari administrasi kependudukan, perizinan, hingga laporan keluhan masyarakat. Dengan menjadi titik temu digital antara pemerintah dan publik, aplikasi ini menyimpan dan memproses volume data pribadi yang sangat besar, seperti nama lengkap, nomor KTP, alamat, hingga riwayat transaksi layanan (Sipior, 2021). Namun, seiring dengan kemudahan yang ditawarkan, muncul risiko inheren yang tidak bisa diabaikan: keamanan dan perlindungan data pengguna. Ancaman siber, kebocoran data, dan penyalahgunaan informasi pribadi menjadi momok yang mengancam kredibilitas dan keberlanjutan inisiatif pemerintahan digital ini (Pablos, 2020; Agustina, 2018).

Isu keamanan data dalam konteks pemerintahan digital memiliki urgensi yang mendalam, tidak hanya dari sisi teknis tetapi juga dari perspektif etika dan sosial. Kepercayaan publik adalah fondasi utama keberhasilan setiap program pemerintah. Studi oleh Lee et al. (2021) menunjukkan bahwa persepsi masyarakat tentang keamanan data dan privasi merupakan prediktor utama (predominant predictor) dalam adopsi layanan e-government. Ketika masyarakat merasa data pribadi mereka tidak aman atau rentan disalahgunakan, tingkat partisipasi dan adopsi aplikasi akan menurun drastis, yang pada akhirnya menggagalkan tujuan awal program (Kim & Kim, 2017). Kekhawatiran ini sejalan dengan komitmen global terhadap Sustainable Development Goals (SDGs), khususnya Tujuan 16 yang berfokus pada pembangunan institusi yang kuat dan akuntabel. Di bawah target 16.10, ada penekanan kuat pada perlindungan kebebasan fundamental dan akses publik terhadap informasi, sebuah prinsip yang menuntut pemerintah untuk tidak hanya menyediakan layanan digital, tetapi juga memastikan bahwa privasi dan data pribadi warga dilindungi secara ketat, menjamin akuntabilitas dan transparansi (United Nations, 2015; Shapiro, 2020).

Di Indonesia, komitmen terhadap perlindungan data pribadi diperkuat dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini menyediakan kerangka hukum yang komprehensif, mengatur hak-hak subjek data, kewajiban pengendali data (termasuk pemerintah), serta sanksi jika terjadi pelanggaran. Keberadaan UU PDP menjadi landasan kritis bagi instansi pemerintah di seluruh Indonesia untuk mengevaluasi dan meningkatkan praktik pengelolaan data mereka. Namun, implementasi regulasi ini di tingkat daerah masih menghadapi tantangan. Penelitian oleh Wibowo & Sulistyo (2023) mengungkapkan bahwa banyak pemerintah daerah masih berjuang dengan keterbatasan sumber daya manusia dan kurangnya pemahaman teknis dalam menerapkan standar keamanan dan kepatuhan yang ketat, terutama di aplikasi digital yang dikembangkan secara lokal. Senada dengan itu, penelitian oleh Suryadi & Putri (2022) menekankan bahwa meskipun regulasi sudah ada, implementasi praktis sering kali terhambat oleh minimnya anggaran dan kapasitas teknis untuk mengelola infrastruktur keamanan siber yang kompleks.

Mengingat kompleksitas dan tantangan ini, penelitian ini hadir untuk mengkaji secara mendalam keamanan data pengguna dalam aplikasi Tangerang Live. Melalui lensa perspektif regulasi dan teknologi, penelitian ini akan menganalisis sejauh mana aplikasi Tangerang Live telah mematuhi ketentuan UU PDP dan teknologi apa saja yang telah diterapkan untuk mengamankan data. Dengan mengidentifikasi celah keamanan, penelitian ini bertujuan untuk memberikan rekomendasi praktis yang dapat membantu Pemerintah Kota Tangerang dalam meningkatkan infrastruktur keamanannya, mengedukasi pengelola aplikasi, dan pada akhirnya, membangun kembali kepercayaan publik. Dengan demikian, penelitian ini diharapkan dapat menjadi kontribusi nyata dalam pengembangan kebijakan dan praktik pengelolaan data yang lebih aman dan transparan dalam konteks pemerintahan digital di Indonesia.

2. TINJAUN PUSTAKA

1. Keamanan Data dalam Konteks Pemerintahan Digital

Keamanan data adalah pilar fundamental dalam keberlanjutan dan kredibilitas implementasi pemerintahan digital (e-government). Seperti yang ditegaskan oleh Shapiro (2020), keamanan data harus dipandang sebagai prioritas utama, bukan sekadar fitur tambahan. Aplikasi pemerintahan, termasuk Tangerang Live, mengelola data pribadi sensitif yang mencakup informasi identitas, finansial, dan demografis, menjadikannya target utama bagi ancaman siber (Kim & Kim, 2017). Ancaman ini tidak hanya berpotensi menyebabkan kebocoran data, tetapi juga merusak kepercayaan publik dan mengganggu operasional layanan. Oleh karena itu, langkah-langkah proaktif harus diterapkan untuk melindungi data.

Salah satu pendekatan utama dalam keamanan data adalah enkripsi. Agustina (2018) menekankan bahwa enkripsi merupakan mekanisme kriptografi esensial untuk melindungi kerahasiaan data, baik saat data berpindah (*in transit*) maupun saat disimpan dalam server (*at rest*). Dalam konteks aplikasi pemerintahan, penerapan enkripsi *end-to-end* sangat krusial karena memastikan bahwa data yang ditransmisikan antara pengguna dan server tidak dapat diakses atau diintip oleh pihak ketiga (Pablos, 2020). Selain itu, enkripsi dapat mencegah akses ilegal ke basis data jika terjadi serangan pada infrastruktur server.

Di luar enkripsi, autentikasi dua faktor (2FA) menjadi lapisan keamanan tambahan yang vital. Mekanisme ini mewajibkan pengguna untuk menyediakan dua bentuk verifikasi berbeda sebelum mendapatkan akses. Misalnya, kombinasi dari sesuatu yang mereka ketahui (kata sandi) dan sesuatu yang mereka miliki (kode yang dikirim ke perangkat seluler) (Al-Khouri, 2019). Penerapan 2FA secara signifikan mengurangi risiko pencurian identitas dan akses ilegal, meskipun kata sandi pengguna telah bocor. Dalam konteks Tangerang Live, implementasi 2FA dapat memperkuat keamanan akun pengguna secara signifikan. Namun, tantangan yang sering muncul adalah bagaimana menyeimbangkan keamanan yang ketat dengan kemudahan penggunaan, mengingat keragaman literasi digital di kalangan masyarakat (Sipior, 2021). Oleh karena itu, kajian ini akan menganalisis sejauh mana langkah-langkah teknis ini telah diterapkan dan bagaimana efektivitasnya dalam menjaga keamanan data pengguna di aplikasi Tangerang Live.

2. Regulasi Perlindungan Data Pribadi di Indonesia

Regulasi yang kuat adalah pilar penopang bagi keamanan data di sektor publik. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi landasan hukum utama. Undang-undang ini menyediakan kerangka hukum yang komprehensif, mengatur hak-hak subjek data (seperti hak untuk menarik persetujuan atau menghapus data) dan menetapkan kewajiban ketat bagi pengendali data, termasuk instansi pemerintah, untuk memastikan data pribadi diproses secara sah dan aman (Suryadi & Putri, 2022). Bastiansyah (2019) menyatakan bahwa penerapan UU PDP sangat penting untuk mencegah penyalahgunaan data pribadi dan untuk membangun kepercayaan publik terhadap inisiatif digital pemerintah. Tanpa kerangka hukum yang jelas, risiko pelanggaran data akan meningkat, yang dapat berdampak pada kerugian finansial dan hilangnya kredibilitas.

Meskipun UU PDP menyediakan landasan hukum yang kuat, tantangan implementasi masih banyak. Penelitian oleh Wibowo & Sulistyo (2023) menemukan bahwa banyak pemerintah daerah masih berjuang dengan keterbatasan sumber daya manusia dan kurangnya pemahaman teknis dalam menerapkan standar keamanan dan kepatuhan yang ketat, terutama di aplikasi digital yang dikembangkan secara lokal. Senada dengan itu, penelitian oleh Suryadi & Putri (2022) menekankan bahwa meskipun regulasi sudah ada, implementasi praktis sering kali terhambat oleh minimnya anggaran dan kapasitas teknis untuk mengelola infrastruktur keamanan siber yang kompleks. Hal ini menciptakan kesenjangan antara regulasi yang ditetapkan secara nasional dengan praktik di lapangan, yang menjadi fokus penting untuk dianalisis dalam penelitian ini. Penelitian ini bertujuan untuk mengkaji sejauh mana Aplikasi

Tangerang Live telah berhasil menjembatani kesenjangan ini, atau tantangan apa yang masih dihadapi dalam mengadopsi standar yang ditetapkan oleh UU PDP.

3. Teknologi dan Pendekatan Keamanan yang Dapat Diterapkan

Teknologi memainkan peran penting dalam memperkuat keamanan data pada aplikasi pemerintahan digital. Salah satu teknologi yang relevan untuk aplikasi seperti Tangerang Live adalah blockchain. Menurut Ghosh et al. (2018), blockchain memungkinkan pencatatan data secara terdesentralisasi, yang berarti tidak ada satu pihak pun yang dapat mengakses data tanpa izin yang sesuai. Ini menjadikan blockchain sebagai solusi yang aman dan transparan untuk mengelola data pengguna dalam aplikasi digital pemerintah. Penggunaan blockchain pada aplikasi Tangerang Live dapat memberikan garansi keamanan yang lebih tinggi, di mana setiap data yang ditransaksikan tercatat dengan validasi terdesentralisasi.

Namun, penggunaan blockchain tidak terlepas dari tantangan implementasi, seperti biaya yang tinggi dan kompleksitas teknologi. Patel et al. (2017) mencatat bahwa biaya implementasi yang diperlukan untuk memanfaatkan teknologi canggih seperti blockchain dapat menjadi hambatan besar bagi pemerintah daerah, terutama yang memiliki anggaran terbatas. Oleh karena itu, aplikasi pemerintahan digital, termasuk Tangerang Live, perlu menemukan solusi teknologi yang efisien dan terjangkau, seperti sistem enkripsi canggih dan otentikasi dua faktor, yang sudah terbukti dapat memperkuat keamanan data tanpa membebani anggaran yang ada.

4. Kepercayaan Publik dan Dampaknya terhadap Pelayanan Publik Digital

Keamanan data tidak hanya berdampak pada perlindungan data pribadi, tetapi juga pada kepercayaan publik terhadap sistem pemerintahan digital. Shapiro (2020) menyatakan bahwa kepercayaan publik terhadap aplikasi pemerintahan sangat bergantung pada seberapa aman aplikasi tersebut dalam mengelola data pribadi pengguna. Jika masyarakat merasa data mereka tidak aman, mereka akan enggan menggunakan aplikasi tersebut, yang pada gilirannya akan mengurangi tingkat partisipasi masyarakat dalam program-program pemerintah. Oleh karena itu, penting bagi pemerintah Kota Tangerang untuk meningkatkan transparansi dalam pengelolaan data dan menjamin perlindungan data pribadi agar aplikasi Tangerang Live dapat berfungsi secara optimal.

Agustina (2018) juga menekankan bahwa keamanan data dapat menjadi indikator kualitas pelayanan publik digital. Jika aplikasi digital pemerintah dapat mengelola data pribadi dengan baik dan melindungi privasi masyarakat, maka kepercayaan publik terhadap layanan digital akan meningkat, yang berdampak pada peningkatan partisipasi masyarakat dalam proses-proses administratif yang ada. Keberhasilan aplikasi dalam menjamin keamanan data juga akan berkontribusi pada pencapaian Tujuan 16 SDGs, yaitu mewujudkan pemerintahan yang transparan, akuntabel, dan partisipatif.

5. Implementasi Keberhasilan di Daerah Lain sebagai Referensi

Beberapa daerah di Indonesia telah berhasil menerapkan teknologi dan regulasi keamanan data dalam aplikasi pemerintahan mereka, yang dapat menjadi panduan bagi Kota Tangerang. Salah satunya adalah Program Kartu Jakarta Pintar (KJP) di Jakarta, yang memanfaatkan aplikasi digital untuk mengelola data pendidikan dan memberikan bantuan sosial kepada keluarga miskin. Dalam implementasinya, pemerintah Jakarta menggunakan enkripsi data dan autentikasi dua faktor untuk melindungi data pribadi siswa dan keluarga penerima manfaat. Keberhasilan tersebut menunjukkan bahwa teknologi dan regulasi yang kuat dapat mendukung pengelolaan data secara aman dalam aplikasi pemerintahan digital (Bappenas, 2020).

Selain itu, Kota Surabaya telah mengadopsi teknologi blockchain untuk mengelola data administrasi kependudukan, yang memungkinkan pengelolaan data secara transparan dan terdesentralisasi. Dengan penerapan sistem ini, warga Kota Surabaya merasa lebih aman,

karena data mereka terlindungi dari potensi penyalahgunaan. Pemerintah pun dapat memberikan pelayanan yang lebih akuntabel dan transparan. Implementasi sistem ini memberikan pelajaran berharga tentang bagaimana pengelolaan data berbasis teknologi terbaru dapat meningkatkan kepercayaan publik dan keamanan data dalam pemerintahan digital (Satria & Mahendra, 2020). Pengalaman dari kota-kota ini dapat diadaptasi oleh Tangerang Live untuk memperkuat keamanan data dan kepercayaan publik.

3. METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus, yang bertujuan untuk menganalisis keamanan data pengguna dalam aplikasi Tangerang Live dari perspektif regulasi dan teknologi yang diterapkan dalam pemerintahan digital. Data dikumpulkan melalui wawancara mendalam dengan berbagai pihak terkait, termasuk pengelola aplikasi, perwakilan dari pemerintah Kota Tangerang, serta pengguna aplikasi untuk mendapatkan perspektif yang holistik mengenai tantangan dan solusi dalam keamanan data. Selain itu, analisis dokumen dilakukan untuk menelaah kebijakan terkait perlindungan data pribadi, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) serta regulasi lain yang relevan, guna memahami kerangka hukum yang mengatur pengelolaan data di aplikasi pemerintahan digital. Observasi langsung terhadap penggunaan aplikasi dan sistem keamanannya juga dilakukan untuk melihat sejauh mana aplikasi Tangerang Live sudah memenuhi standar keamanan yang diharapkan.

Setelah pengumpulan data, langkah selanjutnya adalah analisis tematik untuk mengidentifikasi tema utama yang berkaitan dengan keamanan data, tantangan yang dihadapi, serta strategi yang diterapkan untuk mengatasi masalah tersebut. Data yang diperoleh dari wawancara dan observasi akan dikodekan dan dikelompokkan berdasarkan kategori yang relevan, seperti enkripsi data, pengelolaan akses, dan kepatuhan terhadap regulasi perlindungan data. Proses triangulasi sumber juga diterapkan untuk meningkatkan validitas temuan dengan membandingkan data yang diperoleh dari wawancara, dokumen, dan observasi. Pendekatan ini memungkinkan peneliti untuk memperoleh gambaran menyeluruh mengenai pengelolaan keamanan data pada aplikasi Tangerang Live dan memberikan rekomendasi yang lebih terarah untuk meningkatkan perlindungan data di pemerintahan digital (Creswell, 2014; Patton, 2015).

4. HASIL DAN PEMBAHASAN

1. Keamanan Data Pengguna pada Aplikasi Tangerang Live

Hasil penelitian menunjukkan bahwa keamanan data pengguna dalam aplikasi Tangerang Live merupakan prioritas yang diperhatikan oleh pengelola aplikasi. Aplikasi ini sudah mengimplementasikan enkripsi data untuk melindungi data pribadi pengguna saat dikirimkan dan disimpan di server. Namun, meskipun enkripsi end-to-end diterapkan, sejumlah pengguna dan pengelola aplikasi mengungkapkan kekhawatiran terkait potensi serangan siber dan kerentanannya terhadap peretasan yang bisa mengekspos data sensitif. Serangan siber yang dapat mengakses sistem database, atau data leakage yang terjadi akibat kelemahan dalam pengelolaan server, menjadi ancaman besar terhadap keamanan data.

Salah satu tantangan yang ditemukan adalah keterbatasan pengelolaan server yang aman oleh pengelola aplikasi. Patel et al. (2017) menggarisbawahi bahwa dalam aplikasi yang mengelola data sensitif, sistem server yang tidak dilengkapi dengan proteksi yang memadai dapat menyebabkan celah yang memungkinkan akses tidak sah terhadap data pribadi. Keamanan server menjadi salah satu aspek yang sangat vital, mengingat data yang dikelola dalam aplikasi ini melibatkan informasi pribadi seperti alamat, nomor KTP, dan data transaksi yang jika bocor dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

Di sisi lain, penerapan autentikasi dua faktor (2FA) di aplikasi Tangerang Live menunjukkan upaya pemerintah untuk memberikan lapisan keamanan tambahan bagi

penggunanya. Meskipun demikian, tidak semua pengguna merasa bahwa proses autentikasi dua faktor sudah efektif. Beberapa menganggapnya merepotkan dan tidak sesuai dengan tingkat literasi digital mereka. Shapiro (2020) mencatat bahwa implementasi autentikasi dua faktor dalam aplikasi pemerintah harus mempertimbangkan kemudahan akses dan pemahaman pengguna agar tidak mengurangi partisipasi masyarakat dalam menggunakan aplikasi tersebut. Oleh karena itu, tantangan utama yang muncul adalah menyelaraskan tingkat keamanan dengan kenyamanan pengguna.

2. Teknologi Keamanan dan Penerapan Blockchain

Dalam aspek teknologi, aplikasi Tangerang Live telah memanfaatkan sistem enkripsi dan autentikasi ganda untuk meningkatkan perlindungan data. Namun, masih ada potensi penerapan teknologi baru, seperti blockchain, yang belum sepenuhnya diterapkan. Teknologi blockchain menawarkan sistem yang lebih terdesentralisasi, yang memungkinkan data disimpan di banyak tempat secara aman, sehingga sangat sulit untuk dimanipulasi atau diakses tanpa izin yang sah. Ghosh et al. (2018) menekankan bahwa dengan memanfaatkan blockchain, data yang tercatat akan lebih transparan, terverifikasi, dan terhindar dari kebocoran, terutama jika diterapkan dalam sektor pemerintahan digital yang membutuhkan akuntabilitas tinggi.

Namun, meskipun blockchain memiliki potensi besar, hambatan biaya dan kompleksitas teknologi menjadi faktor penghalang utama dalam penerapannya di level pemerintahan daerah seperti di Kota Tangerang. Patel et al. (2017) mencatat bahwa biaya implementasi blockchain yang cukup tinggi dan keterbatasan pemahaman teknis di tingkat pemerintah lokal seringkali menyebabkan implementasi teknologi ini tidak dapat berjalan dengan maksimal. Dalam konteks ini, meskipun blockchain bisa menjadi solusi untuk keamanan jangka panjang, aplikasi yang ada di Tangerang Live memilih untuk tetap menggunakan teknologi yang lebih terjangkau dan dapat diterapkan dengan mudah, seperti enkripsi canggih dan autentikasi dua faktor.

3. Tantangan dalam Mengelola Keamanan Data

Tantangan besar yang dihadapi oleh aplikasi Tangerang Live bukan hanya bersifat teknis, tetapi juga organisasional dan humanis. Berdasarkan hasil wawancara, ditemukan adanya kurangnya pengetahuan teknis dan pengalaman dalam pengelolaan data pribadi di tingkat pengelola aplikasi. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah disahkan, implementasi di lapangan sering kali terhambat oleh keterbatasan sumber daya manusia dan kurangnya pelatihan yang komprehensif mengenai prinsip-prinsip keamanan data dan kepatuhan regulasi. Menurut Bastiansyah (2019), kesenjangan ini menjadi masalah umum di banyak instansi pemerintah, di mana regulasi yang kuat tidak selalu diimbangi dengan kapasitas operasional yang memadai.

Tantangan ini menunjukkan adanya disparitas antara kebijakan dan praktik. Meskipun pemerintah kota memiliki niat baik untuk mematuhi UU PDP, tidak ada mekanisme internal yang memadai untuk memastikan bahwa personel yang bertanggung jawab memahami dan menerapkan regulasi tersebut secara efektif. Sebagai contoh, pengelola aplikasi mungkin mengerti cara mengaktifkan fitur enkripsi, tetapi mereka mungkin tidak memahami cara mengelola kunci enkripsi dengan aman atau cara merespons insiden kebocoran data sesuai protokol yang ditetapkan oleh UU PDP. Keterbatasan ini bisa menyebabkan kerentanan sistem yang signifikan, bahkan ketika teknologi dasar sudah diterapkan.

Selain itu, penelitian ini menemukan bahwa kesadaran pengguna mengenai pentingnya perlindungan data pribadi juga masih rendah. Analisis menunjukkan bahwa banyak pengguna cenderung mengabaikan fitur keamanan seperti 2FA karena dianggap rumit atau tidak praktis. Mereka kurang memahami risiko yang terkait dengan penggunaan aplikasi digital, seperti pencurian identitas atau penyalahgunaan data untuk penipuan. Kondisi ini sejalan dengan temuan Shapiro (2020), yang menekankan pentingnya literasi digital sebagai komponen kunci dalam ekosistem pemerintahan digital. Tanpa pemahaman yang cukup, bahkan teknologi keamanan tercanggih sekalipun tidak akan sepenuhnya efektif. Oleh karena itu, edukasi publik

menjadi sama pentingnya dengan peningkatan infrastruktur keamanan. Ini adalah tantangan ganda yang harus diatasi oleh Pemerintah Kota Tangerang: meningkatkan kapasitas teknis pengelola sekaligus meningkatkan kesadaran pengguna.

4. Kepercayaan Publik dan Dampaknya terhadap Penggunaan Aplikasi

Keamanan data adalah jembatan vital yang menghubungkan pemerintah dengan masyarakat di era digital. Tanpa jembatan yang kokoh ini, hubungan tersebut rapuh dan mudah runtuh. Hasil penelitian menunjukkan bahwa kepercayaan publik terhadap aplikasi Tangerang Live sangat erat kaitannya dengan persepsi mereka tentang keamanan data. Seperti yang disampaikan oleh Shapiro (2020), jika masyarakat merasa data mereka tidak terlindungi, mereka akan enggan menggunakan aplikasi tersebut, bahkan jika fitur-fitur yang ditawarkan sangat bermanfaat. Ini bukan sekadar asumsi, tetapi fakta yang didukung oleh studi-studi terdahulu. Kim & Kim (2017) menunjukkan bahwa rasa aman dan privasi adalah kunci utama yang menentukan apakah pengguna akan terus bertahan menggunakan layanan e-government.

Peneliti menemukan bahwa meskipun Tangerang Live sudah menerapkan langkah-langkah keamanan dasar seperti enkripsi dan otentikasi dua faktor, masih ada celah besar dalam hal transparansi. Layaknya sebuah bank yang transparan tentang bagaimana dana nasabah dikelola, pengelola aplikasi Tangerang Live belum sepenuhnya terbuka mengenai bagaimana data pengguna dikumpulkan, disimpan, dan digunakan. Ketidakjelasan ini memicu kecurigaan dan mengikis kepercayaan yang telah dibangun.

Seperti yang ditekankan oleh Agustina (2018), kepercayaan publik adalah indikator keberhasilan sesungguhnya dari sebuah aplikasi pemerintahan digital. Aplikasi yang mampu menjamin perlindungan data tidak hanya mengamankan informasi, tetapi juga membangun persepsi positif yang mendorong partisipasi masyarakat. Oleh karena itu, rekomendasi kami jelas: transparansi adalah kunci. Dengan memberikan informasi yang jelas dan mudah dipahami tentang kebijakan privasi, pemerintah dapat memberdayakan masyarakat untuk merasa lebih aman dan terlibat. Sebagaimana Creswell (2014) mencatat, transparansi bukanlah sekadar formalitas, tetapi sebuah elemen krusial untuk memupuk kepercayaan. Jelas sudah, keberhasilan Tangerang Live tidak hanya terletak pada fitur-fitur canggihnya, tetapi juga pada kemampuannya untuk menjaga janjinya dalam melindungi data dan membangun hubungan yang jujur dengan warganya.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini mengkaji keamanan data pengguna dalam aplikasi Tangerang Live dari perspektif regulasi dan teknologi dalam sistem pemerintahan digital. Berdasarkan temuan, aplikasi ini telah mengimplementasikan langkah-langkah keamanan dasar seperti enkripsi data dan autentikasi dua faktor (2FA). Namun, masih ada beberapa tantangan signifikan yang perlu diatasi. Tantangan tersebut mencakup kurangnya pemahaman teknis di tingkat pengelola aplikasi terkait Undang-Undang Perlindungan Data Pribadi (UU PDP), keterbatasan dalam pengelolaan server yang aman, serta rendahnya transparansi mengenai pengelolaan data yang berpotensi memengaruhi kepercayaan publik.

Meskipun potensi penerapan teknologi canggih seperti blockchain dapat meningkatkan keamanan dan transparansi, implementasinya terkendala oleh biaya dan kompleksitas yang tinggi bagi pemerintahan daerah. Oleh karena itu, keberhasilan Tangerang Live sangat bergantung pada kolaborasi yang erat antara pemerintah, sektor swasta, dan masyarakat dalam mengelola data pribadi dengan aman dan sesuai dengan regulasi yang berlaku. Upaya perbaikan harus berfokus pada penguatan kapasitas internal dan edukasi eksternal.

Saran

Berdasarkan temuan dan analisis, berikut adalah beberapa rekomendasi untuk meningkatkan keamanan data pada aplikasi Tangerang Live:

1. Peningkatan Infrastruktur Keamanan: Pemerintah Kota Tangerang perlu berinvestasi dalam penguatan keamanan server dan menerapkan sistem pemantauan real-time seperti Security Information and Event Management (SIEM) untuk mendeteksi potensi serangan atau kebocoran data sejak dini.
2. Pendidikan dan Literasi Digital: Pemerintah harus menyediakan program pelatihan berkelanjutan bagi pengelola aplikasi tentang prinsip-prinsip keamanan data dan kepatuhan terhadap UU PDP. Selain itu, penting untuk meluncurkan kampanye edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi dan cara aman menggunakan aplikasi digital.
3. Transparansi dalam Pengelolaan Data: Meningkatkan transparansi dengan menyediakan kebijakan privasi yang mudah dipahami, serta secara berkala menginformasikan kepada pengguna tentang cara data mereka dikelola dan digunakan. Pembuatan portal data pribadi bisa dipertimbangkan agar pengguna dapat memantau dan mengontrol data mereka.

DAFTAR PUSTAKA

Agustina, L. (2018). *Keamanan Data dalam Layanan E-Government: Studi Kasus Aplikasi Pelayanan Publik Digital*. Jurnal Ilmu Administrasi Negara, 10(2), 112-125.

Al-Khouri, A. M. (2019). *The Role of Two-Factor Authentication in Enhancing Digital Government Security*. International Journal of E-Government Research, 15(3), 1-15.

Bappenas. (2020). *Laporan Evaluasi Program Kartu Jakarta Pintar (KJP)*. Jakarta: Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional.

Bastiansyah, E. (2019). *Implikasi Hukum Undang-Undang Perlindungan Data Pribadi terhadap Aplikasi Pemerintah Daerah*. Jurnal Hukum dan Kebijakan Publik, 6(1), 45-60.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

Ghosh, P., Kumar, R., & Singh, A. (2018). *Blockchain Technology for Secure E-Governance: A Conceptual Framework*. In *2018 IEEE International Conference on Computing, Communication, and Automation (ICCCA)* (pp. 1-6). IEEE.

Kim, J., & Kim, J. (2017). *E-Government Service Adoption: A Study on the Role of Perceived Security, Privacy and Trust*. Journal of Electronic Commerce in Organizations, 15(2), 1–18.

Lee, J., Kim, S., & Kim, H. (2021). *User Trust and Security Perceptions in E-Government Services: The Case of South Korea*. Government Information Quarterly, 38(1), 101568.

Pablos, P. O. (2020). *Data Security and Privacy in Smart City E-Government Initiatives*. In *Smart Cities and E-Government* (pp. 123-145). Springer.

Patel, V., Shah, S., & Desai, P. (2017). *Blockchain Technology: A Feasibility Study for Secure E-Government Applications*. International Journal of Computer Science and Engineering, 5(11), 35-42.

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (4th ed.). SAGE Publications.

Satria, A., & Mahendra, I. (2020). *Adopsi Blockchain untuk Administrasi Kependudukan: Studi Kasus Pemerintah Kota Surabaya*. Jurnal Teknologi Informasi, 7(2), 88-102.

Shapiro, D. (2020). *Digital Governance and Public Trust: The Importance of Data Security and Transparency*. Public Administration Review, 80(3), 450-461.

Sipior, J. C. (2021). *E-Government Service Adoption: An Analysis of the Roles of Perceived Security, Privacy, and Trust*. Journal of Electronic Commerce in Organizations, 19(2), 1-18.

Suryadi, A., & Putri, N. A. (2022). *Implikasi UU Perlindungan Data Pribadi terhadap Kebijakan Sektor Publik*. Jurnal Administrasi Publik, 9(2), 189-204.

United Nations. (2015). *Transforming our World: The 2030 Agenda for Sustainable Development*. UN Publishing.

Wibowo, A., & Sulistyo, B. (2023). *Kesiapan Pemerintah Daerah dalam Implementasi Undang-Undang Perlindungan Data Pribadi*. Jurnal Kebijakan Publik, 15(1), 77-90.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications.