JIAP | Jurnal Ilmu Administrasi Publik
ISSN 2339-2932 | FISIP UM Mataram
Vol. 13 No. 2 September 2025, Hal. 156-172

KEAMANAN DATA SEBAGAI PILAR STRATEGIS PERCEPATAN TRANSFORMASI DIGITAL PEMERINTAH KOTA MAKASSAR

Erni Salijah[a1*], Abdul Basid [b2], Aswar Annas [c3]

[1,2,3]Universitas Pepabri Makassar, Jl. Letjen Hertasning No.106, Kota Makassar, 90222, Indonesia
ernisalijah2019@gmail.com*

INFO ARTIKEL

Riwayat Artikel:

Diterima: 23-08-2025
Disetujui: 12-09-2025
Dipublikasikan: 29-09-2025

Kata Kunci:

1. Keamanan data
2. Upaya pemerintah
3. Transformasi digital
4. Kebijakan publik
5. Layanan publik

Keywords:

1. Data security
2. Government efforts
3. Digital transformation
4. Public policy
5. Public services

ABSTRAK

Abstrak: Di tengah perkembangan era digital, risiko kebocoran data kian meningkat dengan karakter yang semakin rumit, sehingga berpotensi mengganggu aspek kerahasiaan, keakuratan, dan aksesibilitas informasi. Urgensi masalah keamanan data dan informasi di Kota Makassar dalam konteks percepatan transformasi digital mencerminkan perlunya respons proaktif untuk melindungi kerahasiaan, integritas, dan ketersediaan data dari ancaman yang semakin kompleks. Tujuan penelitian ini adalah untuk mengidentifikasi upaya yang dilakukan pemerintah dalam meningkatkan keamanan informasi, serta untuk memetakan hambatan yang dihadapinya. Studi ini menggunakan pendekatan kualitatif, dengan mengumpulkan data melalui beberapa teknik, termasuk wawancara, dokumentasi, dan observasi. Informan kunci terdiri dari para pejabat dan staf di Dinas Komunikasi dan Informatika Kota Makassar yang memiliki pemahaman yang mendalam tentang kebijakan, praktik, dan infrastruktur terkait keamanan data dan informasi. Temuan utama dari upaya pemerintah Kota Makassar dalam meningkatkan efektivitas keamanan data dan informasi meliputi empat aspek krusial yaitu penguatan infrastruktur keamanan, pelatihan pegawai, sosialisasi publik, serta monitoring dan evaluasi berkala. Tantangan utama yang dihadapi termasuk evolusi ancaman siber, keterbatasan anggaran, kurangnya kesadaran pegawai, kompleksitas regulasi, dan integrasi sistem. Rekomendasi untuk mengatasi tantangan tersebut mencakup penerapan prinsip keamanan berlapis, manajemen anggaran berbasis risiko, peningkatan pelatihan, pematuhan regulasi, dan desain sistem yang mendukung integrasi. Mengadopsi pendekatan berbasis risiko dan standar internasional juga dapat membantu meningkatkan keamanan, membangun kepercayaan publik, dan mendukung transformasi digital yang aman dan efisien di Kota Makassar.

Abstract: *In the midst of the development of the digital era, the risk of data leaks is increasing with increasingly complex characters, thus potentially disrupting aspects of confidentiality, accuracy, and accessibility of information. The urgency of data and information security issues in Makassar City in the context of accelerating digital transformation reflects the need for a proactive response to protect the confidentiality, integrity, and availability of data from increasingly complex threats. This research aims to identify the efforts made by the government to improve information security, as well as to map the obstacles it faces. This study uses a qualitative approach, collecting data through several techniques, including interviews, documentation, and observation. Key informants consist of officials and staff at the Makassar City Communications and Information Service who have a deep understanding of policies, practices, and infrastructure related to data and information security. The main findings from the Makassar City government's efforts to increase the effectiveness of data and information security include four crucial aspects, namely strengthening security infrastructure, employee training, public outreach, and regular monitoring and evaluation. Critical challenges faced include the evolution of cyber threats, budget constraints, lack of employee awareness, regulatory complexity, and system integration. Recommendations to address these challenges include implementing layered security principles, risk-based budget management, improving training, regulatory compliance, and system design that supports integration. Adopting a risk-based approach and international standards can also help improve security, build public trust, and support safe and efficient digital transformation in Makassar City.*

PENDAHULUAN

Dalam era digital saat ini, rentang kebocoran informasi menjadi semakin luas dan kompleks, mengancam kerahasiaan, integritas, dan ketersediaan data (Mohd & Yunos, 2020). Masalah kebocoran data dan informasi telah diidentifikasi di Indonesia, termasuk di Kota Makassar (Aldifansa, Wicaksono, Nurfadilah, Santoso Gunawan, & Edbert, 2023). Oleh karena itu, Dinas Komunikasi dan Informatika Kota Makassar telah mengambil langkah-langkah proaktif untuk melindungi informasi sensitif dengan menggelar Bimbingan Teknis tentang pengembangan sandi serta penerapan dan penilaian mandiri indeks keamanan informasi (Fatir, 2019). Urgensi dari masalah ini tidak dapat diabaikan, mengingat dampak yang bisa merugikan baik bagi individu maupun institusi, termasuk potensi kehilangan data sensitif, pelanggaran privasi, dan bahkan ancaman terhadap stabilitas sistem secara keseluruhan (Golightly et al., 2022). Oleh karena itu, langkah-langkah perlindungan dan kesadaran akan keamanan informasi merupakan hal yang mendesak untuk diimplementasikan guna memitigasi risiko-risiko tersebut (Ren et al., 2022).

Kelemahan dalam keamanan data dan informasi secara umum dapat memiliki dampak yang merugikan dalam berbagai aspek kehidupan. Secara ekonomi, lemahnya keamanan data dapat mengakibatkan kerugian finansial yang signifikan baik bagi individu maupun organisasi, melalui pencurian identitas, penipuan keuangan, atau penyalahgunaan informasi sensitif lainnya (Vrhovec & Markelj, 2018). Di sisi lain, dalam ranah sosial dan politik, kebocoran data dapat memicu kekhawatiran akan privasi individu (Pham, Phan, Trinh, Mai, & Le, 2023), meningkatkan risiko kejahatan cyber (Chadwick et al., 2020), dan bahkan merusak kepercayaan publik terhadap lembaga atau entitas yang terlibat (Kang & Deng, 2023). Lebih lanjut lagi, lemahnya keamanan data juga dapat mengganggu operasi bisnis, menghambat inovasi, dan mengancam stabilitas infrastruktur kritis seperti sistem energi atau transportasi (Haghighi, Farivar, Jolfaei, Asl, & Zhou, 2023). Dengan demikian, pentingnya meningkatkan keamanan data dan informasi tidak hanya relevan dalam konteks teknologi, tetapi juga memiliki implikasi yang luas dalam menjaga stabilitas dan kesejahteraan masyarakat secara keseluruhan.

Respons pemerintah melalui kebijakan dan infrastruktur yang terarah, sangat penting dalam mengatasi tantangan yang ditimbulkan oleh kelemahan dalam keamanan data dan informasi (Arunprasath & Annamalai, 2024). Pemerintah memiliki tanggung jawab utama untuk melindungi warganya dari ancaman cyber yang semakin kompleks, dan hal ini memerlukan adopsi kebijakan yang komprehensif untuk menetapkan standar keamanan yang ketat, menegakkan regulasi yang relevan, serta memperkuat infrastruktur teknologi yang mampu menghadapi dan merespons ancaman tersebut (S. Sharma, Rahaman, & Sinha, 2021). Respons pemerintah yang terkoordinasi dan proaktif akan membantu membangun lingkungan yang aman dan andal bagi penggunaan teknologi informasi dan komunikasi, serta memastikan perlindungan data dan privasi bagi seluruh masyarakat (Xia, Semirumi, & Rezaei, 2023).

Transformasi digital dalam pemerintahan merujuk pada adopsi teknologi digital untuk meningkatkan efisiensi, transparansi, dan kualitas layanan publik (Kristensen & Andersen, 2023). Prospek dari transformasi

digital dalam pemerintahan sangat menjanjikan. Dengan pemanfaatan teknologi seperti big data, kecerdasan buatan, dan sistem informasi berbasis cloud, pemerintah dapat mengelola dan menganalisis data lebih efektif, memungkinkan pengambilan keputusan yang lebih baik dan responsif terhadap kebutuhan masyarakat (Scupola & Mergel, 2022). Implementasi teknologi ini berpotensi untuk mengurangi birokrasi, mempercepat proses administratif, serta meningkatkan akuntabilitas dan keterbukaan informasi publik.

Secara teoritik, transformasi digital dalam pemerintahan dapat dijelaskan melalui teori adopsi teknologi, yang mencakup faktor-faktor seperti dorongan internal dan eksternal, kesiapan organisasi, dan dampak potensial terhadap stakeholders. Teori ini menyatakan bahwa adopsi teknologi digital memerlukan kesiapan infrastruktur, perubahan dalam budaya organisasi, serta pelatihan dan pengembangan kompetensi bagi pegawai. Faktor-faktor ini mempengaruhi bagaimana dan seberapa cepat teknologi diimplementasikan dan diterima dalam sistem pemerintahan (Yuan et al., 2023). Implementasi transformasi digital memerlukan strategi yang terencana dengan baik, yang mencakup perencanaan teknologi, manajemen perubahan, dan keterlibatan stakeholders. Penting bagi pemerintah untuk mengembangkan kerangka kerja yang jelas dan menetapkan tujuan yang terukur untuk proyek-proyek digitalisasi. Implementasi juga harus melibatkan pelatihan untuk pegawai, pembaruan infrastruktur teknologi, serta pengembangan kebijakan untuk melindungi data dan privasi. Keterlibatan publik dalam proses ini juga penting untuk memastikan bahwa teknologi yang diterapkan sesuai dengan kebutuhan dan harapan masyarakat (Baharuddin, 2020; Ibrahim, Baharuddin, & Wance, 2023; Isabella, Agustian, Baharuddin, & Ibrahim, 2025; Isabella, Alfitri, Saptawan, Nengyanti, & Baharuddin, 2024).

Keamanan data dan informasi merupakan aspek krusial dalam era digitalisasi yang semakin berkembang (Fisdian Adni, Rusadi, & Baharuddin, 2024). Dengan meningkatnya penggunaan teknologi informasi, risiko terhadap data pribadi dan informasi sensitif juga meningkat (Sarkar & Das, 2022). Serangan siber, kebocoran data, dan penyalahgunaan informasi dapat menimbulkan dampak serius bagi individu dan organisasi (Alharbi, Halikias, Rajarajan, & Yamin, 2021). Oleh karena itu, penting bagi pemerintah dan sektor swasta untuk menerapkan kebijakan keamanan data yang ketat, termasuk enkripsi data, autentikasi yang kuat, serta pengawasan dan audit rutin. Kebijakan ini harus mencakup perlindungan terhadap data pribadi, pengaturan akses, dan mekanisme untuk merespons insiden keamanan dengan cepat dan efektif.

Di samping itu, pendidikan dan pelatihan mengenai keamanan data untuk karyawan dan pengguna juga sangat penting. Kesadaran dan pemahaman tentang potensi ancaman serta langkah-langkah pencegahan dapat membantu mengurangi risiko. Selain itu, regulasi yang ketat dan kepatuhan terhadap standar internasional seperti General Data Protection Regulation (GDPR) di Eropa dapat memperkuat perlindungan data dan informasi (Hoofnagle, Sloot, & Borgesius, 2019). Dengan pendekatan yang komprehensif dalam manajemen keamanan data, baik secara teknis maupun operasional, organisasi dapat melindungi integritas dan kerahasiaan data, serta membangun kepercayaan pengguna dan publik.

Pengembangan infrastruktur adalah kunci untuk mendukung transformasi digital dan memastikan keberhasilan implementasi teknologi. Secara teoritik, infrastruktur digital mencakup berbagai komponen

seperti jaringan komunikasi, pusat data, perangkat keras, dan perangkat lunak yang saling terintegrasi untuk mendukung operasional dan layanan digital (R. Sharma, Fantin, Prabhu, Guan, & Dattakumar, 2016). Ini menjelaskan bahwa pengembangan infrastruktur harus dimulai dengan perencanaan dan desain yang matang, diikuti dengan penerapan dan pemeliharaan yang efektif. Infrastruktur yang baik mendukung kinerja sistem informasi, memungkinkan skalabilitas, dan memastikan keterhubungan yang stabil serta keamanan data yang memadai.

Dalam konteks pengembangan infrastruktur, teori adopsi teknologi juga relevan. Menurut teori ini, kesiapan infrastruktur merupakan faktor determinan dalam adopsi teknologi baru (X. Chen, Tang, & Xu, 2023). Infrastruktur yang tidak memadai dapat menghambat implementasi teknologi dan mengurangi efisiensi operasional. Oleh karena itu, investasi dalam pengembangan infrastruktur, seperti peningkatan kapasitas server, perluasan jaringan, dan pembaruan perangkat keras, menjadi sangat penting. Infrastruktur yang handal mendukung keberlangsungan layanan digital dan meningkatkan kapasitas organisasi dalam menghadapi tuntutan dan perubahan teknologi yang cepat, serta membantu organisasi dalam memanfaatkan peluang digital secara optimal.

Secara keseluruhan, transformasi digital dalam pemerintahan menawarkan prospek yang signifikan untuk meningkatkan efisiensi, transparansi, dan kualitas layanan publik. Keberhasilan implementasinya sangat bergantung pada kesiapan infrastruktur, keamanan data, dan strategi yang terencana dengan baik. Penerapan teknologi digital harus disertai dengan pengembangan infrastruktur yang memadai dan kebijakan keamanan yang ketat untuk melindungi data sensitif. Selain itu, keterlibatan stakeholders dan pelatihan yang efektif juga memainkan peran penting dalam memastikan adopsi teknologi yang sukses dan bermanfaat bagi masyarakat. Dengan pendekatan yang holistik dan terintegrasi, pemerintah dapat memanfaatkan potensi transformasi digital untuk mencapai tata kelola yang lebih baik dan pelayanan publik yang lebih responsif.

Urgensi untuk menangani tantangan keamanan data dan informasi dalam percepatan transformasi digital di Kota Makassar sangatlah mendesak. Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi, rentang kebocoran informasi menjadi semakin kompleks dan berpotensi merugikan baik individu maupun institusi. Potensi kehilangan data sensitif, pelanggaran privasi, serta ancaman terhadap stabilitas sistem mendorong perlunya respons cepat dan efektif dari pemerintah setempat. Langkah-langkah proaktif dalam pengembangan kebijakan dan infrastruktur yang responsif menjadi kunci untuk meminimalkan risiko dan memastikan keamanan informasi di tengah transformasi digital yang pesat. Dalam menangani tantangan keamanan data dan informasi dalam konteks percepatan transformasi digital di Kota Makassar, pendekatan pemecahan masalah yang efektif melibatkan beberapa langkah kunci. Pertama, perlu dilakukan evaluasi mendalam terhadap langkah-langkah proaktif yang telah diambil oleh Dinas Komunikasi dan Informatika, termasuk efektivitas dari Bimbingan Teknis dan implementasi indeks keamanan informasi. Selanjutnya, diperlukan kerja sama lintas sektor dan konsultasi dengan pakar keamanan *cyber* untuk mengidentifikasi celah keamanan yang mungkin terlewatkan serta mengembangkan solusi yang responsif.

Langkah-langkah ini harus disertai dengan pembaruan kebijakan yang relevan dan perkuatan infrastruktur teknologi yang mampu menghadapi ancaman cyber yang semakin berkembang. Dengan pendekatan ini, diharapkan dapat tercipta lingkungan yang aman dan andal bagi transformasi digital yang berkelanjutan di Kota Makassar.

Perbedaan utama studi ini dengan penelitian-penelitian sebelumnya terletak pada fokus kajian yang tidak hanya membahas keamanan data dari sisi teknis atau risiko siber, tetapi mengaitkannya secara langsung dengan strategi percepatan transformasi digital di tingkat pemerintah daerah, khususnya Pemerintah Kota Makassar. Studi terdahulu cenderung menyoroti isu keamanan data dalam konteks umum seperti perlindungan privasi, risiko kejahatan siber, atau penguatan infrastruktur teknologi secara teknis, tanpa mengaitkannya dengan bagaimana keamanan data menjadi elemen kunci keberhasilan implementasi kebijakan digital dan peningkatan kualitas layanan publik yang responsif. Kebaruan (novelty) penelitian ini terletak pada pendekatan integratif yang mengkaji keamanan data sebagai *strategic enabler* transformasi digital melalui analisis kebijakan, kesiapan infrastruktur, tata kelola keamanan informasi, serta partisipasi stakeholder dalam memperkuat indeks keamanan informasi daerah. Dengan demikian, studi ini tidak hanya memberikan kontribusi teoritis mengenai hubungan erat antara keamanan data dan transformasi digital, tetapi juga menawarkan model implementasi kebijakan yang dapat direplikasi untuk mempercepat agenda *smart governance* di pemerintah daerah lainnya.

Rumusan masalah dalam konteks ini dapat difokuskan pada dua pertanyaan penelitian utama: Pertama, bagaimana Dinas Komunikasi dan Informatika Kota Makassar dapat meningkatkan efektivitas langkah-langkah proaktif yang telah diambil dalam melindungi informasi sensitif, termasuk melalui penyelenggaraan Bimbingan Teknis dan penerapan indeks keamanan informasi? Kedua, bagaimana tantangan yang dirasakan oleh pemerintah dalam upaya menjaga efektifitas keamanan data dan informasi? Implikasi temuan dari penelitian ini diharapkan dapat memberikan panduan bagi pemerintah setempat dalam meningkatkan keamanan informasi, melindungi masyarakat dari ancaman cyber, serta memperkuat infrastruktur teknologi untuk mendukung transformasi digital yang berkelanjutan dan aman.

METODE PENELITIAN

Studi ini menggunakan pendekatan kualitatif untuk mengumpulkan data melalui beberapa teknik, termasuk wawancara, dokumentasi, dan observasi. Informan kunci terdiri dari para pejabat dan staf di Dinas Komunikasi dan Informatika Kota Makassar yang memiliki pemahaman yang mendalam tentang kebijakan, praktik, dan infrastruktur terkait keamanan data dan informasi. Wawancara digunakan untuk mendapatkan pandangan dan pengalaman langsung dari informan kunci, sementara dokumentasi digunakan untuk menganalisis kebijakan, pedoman, dan dokumen terkait keamanan informasi. Observasi membantu dalam memahami implementasi kebijakan dan praktik keamanan di lapangan. Dengan kombinasi metode ini, diharapkan studi ini dapat memberikan pemahaman yang komprehensif tentang status dan tantangan keamanan data dan informasi di tingkat lokal.

Data yang diperoleh dari wawancara, dokumentasi, dan observasi ditranskripsikan secara cermat dan dipindahkan ke dalam alat analisis NVivo 12 Plus untuk proses analisis yang sistematis dan terstruktur. NVivo 12 Plus dipilih karena kemampuannya untuk melakukan analisis mendalam dan memvisualisasikan data kualitatif dengan fitur-fitur canggihnya (Salahudin, Nurmandi, & Loilatu, 2020). Unit analisis cases classification digunakan untuk mengelompokkan dan menganalisis data berdasarkan kategori atau kasus tertentu, memungkinkan identifikasi pola dan perbedaan di antara unit-unit yang dianalisis. Pendekatan ini memudahkan penyusunan dan perbandingan data dalam konteks yang lebih terstruktur dan relevan dengan tujuan penelitian.

Validasi data secara teoritik mencakup penggunaan triangulasi untuk meningkatkan kredibilitas temuan dengan membandingkan informasi dari berbagai sumber, sehingga mengurangi bias dan meningkatkan keandalan data. Pembuatan kode yang tepat dan akurat dalam proses analisis kualitatif membantu mengorganisir data secara sistematis, memudahkan identifikasi tema dan pola yang konsisten. Teknik validasi silang antara peneliti memastikan kesesuaian interpretasi dengan mengevaluasi konsistensi dan objektivitas analisis, sehingga memperkuat validitas dan keandalan kesimpulan yang dihasilkan.

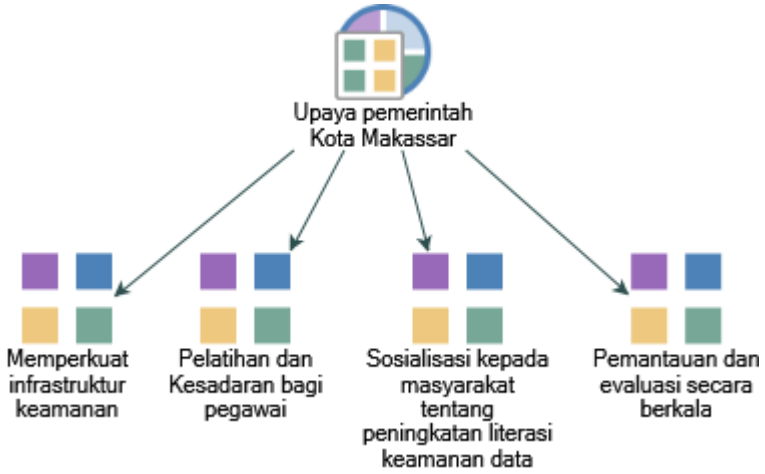
Sebagai penutup, penelitian ini merupakan jenis penelitian kualitatif yang berfokus pada pemahaman mendalam terhadap fenomena keamanan data dan percepatan transformasi digital di tingkat pemerintah daerah. Jenis data yang digunakan adalah data primer yang diperoleh langsung dari wawancara dan observasi, serta data sekunder yang berasal dari berbagai dokumen resmi, kebijakan, dan arsip terkait keamanan informasi. Narasumber utama terdiri dari pejabat dan staf Dinas Komunikasi dan Informatika Kota Makassar yang memiliki peran strategis dalam perencanaan dan implementasi kebijakan keamanan data. Teknik pengumpulan data meliputi wawancara mendalam, observasi partisipatif, dan studi dokumentasi untuk menghasilkan gambaran komprehensif mengenai kondisi aktual di lapangan. Selanjutnya, teknik analisis data dilakukan menggunakan perangkat lunak NVivo 12 Plus melalui proses koding, kategorisasi, visualisasi, dan triangulasi guna memastikan objektivitas, kedalaman, dan validitas hasil penelitian.

HASIL DAN PEMBAHASAN

Upaya Pemerintah: Meningkatkan efektivitas keamanan data dan informasi dalam percepatan transformasi digital DI Kota Makassar

Meningkatkan efektivitas keamanan data dan informasi dalam percepatan transformasi digital di Kota Makassar menjadi sangat penting karena kota ini sedang berkembang pesat dalam mengadopsi teknologi digital untuk pelayanan publik. Dalam era digitalisasi yang semakin maju, risiko terhadap keamanan data seperti serangan siber dan kebocoran informasi juga meningkat. Pemerintah harus memastikan infrastruktur keamanan yang kuat agar data pribadi masyarakat dan informasi penting pemerintah terlindungi dengan baik. Selain itu, keamanan yang efektif akan membangun kepercayaan masyarakat terhadap layanan digital pemerintah, sehingga mempercepat proses transformasi digital secara keseluruhan di Kota Makassar.

Ada beberpa upaya yang telah dilakukan pemerintah Kota Makassar untuk meningkatkan efektivitas keamanan data dan informasi dalam percepatan transformasi digital. Ini dapat dicermati pada Gambar 1.



Gambar 1. Upaya pemerintah Kota Makassar dalam meningkatkan efektivitas keamanan data dan informasi

Sumber: Diolah peneliti dengan Nvivo 12 Plus, 2025

Gambar 1 menegaskan bahwa penguatan infrastruktur keamanan merupakan langkah krusial dalam melindungi data dan informasi dari ancaman siber. Dengan meningkatkan dan memperbarui sistem keamanan siber, seperti penggunaan firewall, enkripsi, dan deteksi intrusi, pemerintah Kota Makassarterus berupaya untuk memperkuat pertahanan terhadap berbagai serangan siber. Firewall berfungsi sebagai penghalang antara jaringan internal dan eksternal, mencegah akses yang tidak sah, sementara enkripsi mengamankan data dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci yang sesuai. Deteksi intrusi, di sisi lain, memungkinkan pemantauan real-time terhadap aktivitas mencurigakan dan potensi serangan, sehingga respons dapat dilakukan segera untuk mengurangi dampak serangan.

Secara teoritik, upaya ini dapat didukung oleh prinsip keamanan informasi yang tertuang dalam model CIA (*Confidentiality*, *Integrity*, *Availability*). Model ini menyarankan bahwa untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data, perlu ada lapisan-lapisan proteksi yang solid. Penggunaan firewall, enkripsi, dan deteksi intrusi secara langsung mendukung prinsip-prinsip ini dengan mencegah akses tidak sah (confidentiality), memastikan data tidak diubah secara tidak sah (integrity), dan mendeteksi serta merespons ancaman dengan cepat untuk menjaga ketersediaan layanan (availability). Implementasi teknologi ini dalam infrastruktur keamanan membantu menciptakan lingkungan yang lebih aman dan stabil untuk proses transformasi digital di Kota Makassar.

Selain itu, pemerintah Kota Makassar juga melakukan pelatihan dan kesadaran untuk pegawai sebagai upaya penting dalam meningkatkan keamanan data dan informasi. Salah satu hal yang dilakukan yaitu melakukan bimbingan teknis bagi pegawai.

Gambar 2. Upaya pemerintah Kota Makassar dalam meningkatkan efektivitas keamanan data dan informasi dengan bimbingan teknis sebagai upaya dari bagian pelatihan dan kesadaran pegawai

Sumber: antaranews.com, 2019

Gambar 2 menunjukkan upaya pemerintah Kota Makassar untuk meningkatkan efektivitas keamanan data dan informasi mencakup langkah-langkah signifikan dalam bimbingan teknis sebagai bagian dari pelatihan dan kesadaran pegawai. Mengingat kerentanan informasi di era digital, Dinas Komunikasi dan Informatika (Dinas Kominfo) Kota Makassar telah mengadakan bimbingan teknis yang fokus pada pengembangan sandi serta penerapan dan penilaian mandiri indeks keamanan informasi. Bimbingan ini bertujuan untuk memperkuat kapasitas pegawai dalam melindungi data dan memastikan bahwa semua sistem dan prosedur keamanan dijalankan dengan efektif (Fatir, 2019).

Dengan melibatkan perwakilan dari berbagai Organisasi Perangkat Daerah di kota Makassar, pemerintah memastikan bahwa pelatihan ini menyentuh berbagai aspek penting dari keamanan informasi. Inisiatif ini tidak hanya memperkuat kesadaran dan keterampilan pegawai dalam mengelola risiko keamanan tetapi juga membangun dasar yang kokoh untuk penilaian mandiri keamanan informasi. Melalui upaya ini, Kota Makassar berharap dapat mengurangi risiko kebocoran data dan meningkatkan ketahanan sistem informasi mereka dalam menghadapi ancaman siber yang terus berkembang. Menyelenggarakan pelatihan reguler mengenai praktik keamanan terbaik, kesadaran tentang ancaman siber, dan cara melindungi data pribadi membantu pegawai dan pengguna sistem memahami potensi risiko dan tindakan pencegahan yang harus diambil. Pelatihan ini tidak hanya memberikan pengetahuan tentang teknologi dan kebijakan keamanan, tetapi juga mengedukasi peserta tentang praktik sehari-hari yang dapat mengurangi risiko, seperti mengidentifikasi email phishing, menggunakan kata sandi yang kuat, dan mengelola akses data secara aman.

Secara teoritik, konsep ini didukung oleh teori keamanan perilaku yang menyatakan bahwa kesadaran dan pengetahuan pengguna berperan signifikan dalam mencegah pelanggaran keamanan. Teori ini

menggarisbawahi pentingnya faktor manusia dalam keamanan informasi, mengingat bahwa banyak insiden keamanan terjadi akibat kesalahan atau kelalaian pengguna (Crossler et al., 2013). Program pelatihan yang efektif dapat meningkatkan kepatuhan terhadap kebijakan keamanan dan mengurangi kesalahan manusia, yang sering menjadi titik lemah dalam sistem keamanan. Dengan meningkatkan kesadaran dan pengetahuan pegawai, organisasi dapat memperkuat lapisan pertahanan keamanan data dan mengurangi kemungkinan terjadinya pelanggaran atau ancaman siber. Di sisi lainnya, pemerintah Kota Makassar juga terus melakukan upaya sosialisasi publik tentang peningkatan literasi keamanan data. Hal ini adalah langkah penting untuk melibatkan masyarakat dalam upaya perlindungan data pribadi dan keamanan siber. Dengan mengedukasi publik mengenai risiko siber, praktik keamanan terbaik, dan cara melindungi informasi pribadi, pemerintah dan organisasi dapat meningkatkan kesadaran dan pengetahuan masyarakat mengenai pentingnya keamanan data. Sosialisasi ini dapat dilakukan melalui kampanye informasi, seminar, pelatihan komunitas, dan distribusi materi edukatif yang mudah dipahami.

Secara teoritik, pendekatan ini didukung oleh teori kesadaran risiko, yang menunjukkan bahwa pemahaman dan pengetahuan tentang risiko dapat mengubah perilaku dan meningkatkan langkah-langkah pencegahan (Y. Chen, kumara, & Sivakumar, 2023). Teori ini menekankan bahwa individu yang sadar akan potensi ancaman dan konsekuensi dari pelanggaran keamanan cenderung lebih proaktif dalam melindungi data pribadi mereka. Sosialisasi publik berfungsi untuk menciptakan budaya keamanan yang lebih baik, di mana masyarakat tidak hanya memahami pentingnya melindungi data tetapi juga aktif dalam menerapkan praktik keamanan yang disarankan. Dengan melibatkan publik dalam literasi keamanan data, risiko pelanggaran dapat dikurangi, dan perlindungan data dapat diperkuat secara keseluruhan.

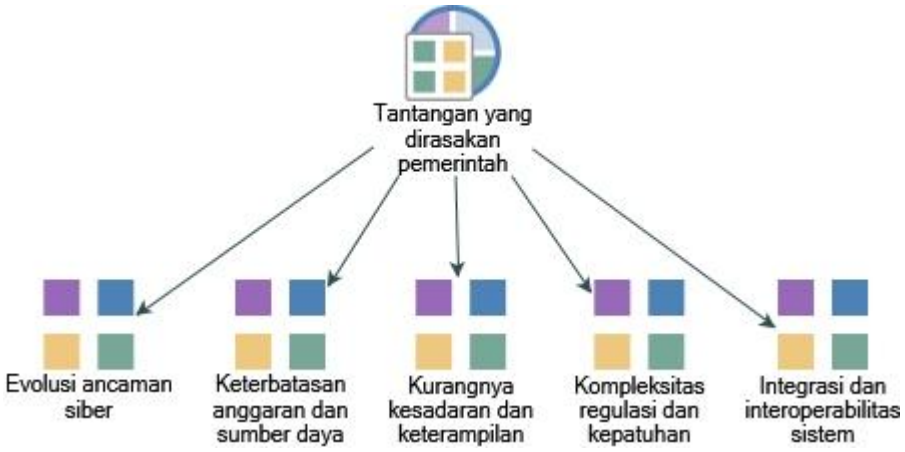
Upaya lainnya yang dilakukan pemerintah Kota Makassar yaitu monitoring dan evaluasi berkala. Hal ini merupakan langkah krusial dalam memastikan efektivitas sistem keamanan data dan informasi. Dengan melakukan pemantauan rutin, organisasi dapat mengidentifikasi potensi kerentanan dan ancaman sebelum mereka menyebabkan kerusakan signifikan. Proses evaluasi ini melibatkan audit keamanan yang mendalam untuk menilai kinerja sistem dan kebijakan yang ada, memastikan bahwa mereka sesuai dengan standar terkini dan perkembangan teknologi. Hal ini juga memungkinkan penyesuaian dan perbaikan berkelanjutan untuk mengatasi kelemahan yang ditemukan dan mengadaptasi terhadap perubahan ancaman.

Secara teoritik, pendekatan ini didukung oleh teori manajemen keamanan informasi yang menekankan pentingnya siklus pemantauan dan evaluasi dalam sistem manajemen risiko (Culot, Nassimbeni, Podrecca, & Sartor, 2021). Teori ini menyarankan bahwa keamanan informasi harus dikelola secara dinamis dan berkelanjutan, mengingat ancaman dan teknologi terus berkembang. Dengan melakukan audit keamanan secara rutin dan menyesuaikan kebijakan berdasarkan hasil evaluasi, organisasi dapat menjaga efektivitas perlindungan data dan memastikan bahwa sistem keamanan tetap relevan dan responsif terhadap tantangan baru. Pendekatan ini juga mendukung prinsip perbaikan berkelanjutan, yang penting untuk mempertahankan tingkat keamanan yang tinggi dalam lingkungan yang terus berubah.

Implikasi yang diharapkan dari upaya pemerintah Kota Makassar ini adalah terciptanya lingkungan digital yang lebih aman dan efektif dalam mendukung transformasi digital. Dengan mengimplementasikan penguatan infrastruktur keamanan, pelatihan pegawai, sosialisasi publik, dan monitoring berkala, diharapkan risiko terhadap data dan informasi dapat diminimalisir secara signifikan. Upaya ini tidak hanya akan memperkuat pertahanan terhadap ancaman siber, tetapi juga meningkatkan kesadaran dan kepatuhan terhadap kebijakan keamanan, serta memastikan bahwa sistem keamanan tetap adaptif dan responsif terhadap perubahan. Hasilnya, pemerintah Kota Makassar dapat mencapai tingkat keamanan data yang tinggi, mendukung keberhasilan transformasi digital, dan meningkatkan kepercayaan masyarakat terhadap pengelolaan data publik.

Tantangan pemerintah dalam upaya menjaga efektifitas keamanan data dan informasi

Diskusi mengenai tantangan pemerintah dalam menjaga efektivitas keamanan data dan informasi sangat penting mengingat peran krusial data dalam operasional dan pelayanan publik. Dengan meningkatnya ketergantungan pada teknologi digital dalam berbagai aspek pemerintahan, keamanan data menjadi kunci utama untuk melindungi integritas, kerahasiaan, dan ketersediaan informasi. Tantangan-tantangan yang dihadapi dalam mengelola keamanan data dan informasi tidak hanya berpotensi menimbulkan risiko terhadap data sensitif dan pribadi tetapi juga dapat mempengaruhi kepercayaan publik dan efisiensi operasional. Memahami dan mengatasi tantangan ini merupakan langkah penting untuk memastikan bahwa sistem keamanan data dapat berfungsi secara optimal dan mendukung tujuan transformasi digital pemerintah dengan efektif dan aman.



Gambar 3. Tantangan pemerintah Kota Makassar dalam upaya menjaga efektifitas keamanan data dan informasi.

Sumber: Diolah peneliti dengan Nvivo 12 Plus, 2025

Gambar 3 menjelaskan tentang tantangan pemerintah dalam upaya menjaga efektivitas keamanan data dan informasi meliputi beberapa aspek penting yang mempengaruhi keberhasilan implementasi dan pemeliharaan sistem keamanan. Pertama, evolusi ancaman siber yang cepat dan kompleks menjadi tantangan utama. Ancaman siber terus berkembang dengan teknik yang semakin canggih, seperti ransomware dan serangan zero-day, yang memerlukan sistem keamanan yang terus diperbarui dan adaptif. Pemerintah harus

mampu mengikuti perkembangan teknologi dan tren ancaman untuk memastikan sistem perlindungan tetap efektif.

Kedua, keterbatasan anggaran dan sumber daya sering kali menjadi hambatan. Pengembangan dan pemeliharaan infrastruktur keamanan siber memerlukan investasi yang besar, dan sering kali anggaran yang tersedia tidak mencukupi untuk memenuhi semua kebutuhan teknologi dan pelatihan. Keterbatasan ini dapat mempengaruhi kemampuan pemerintah untuk menerapkan solusi keamanan yang terbaru dan memadai. Keterbatasan anggaran dan sumber daya dapat mengakibatkan perlambatan dalam pengembangan dan pemeliharaan sistem keamanan yang efektif, serta mengurangi kemampuan untuk merespons ancaman siber dengan cepat. Akibatnya, hal ini dapat meninggalkan celah dalam pertahanan yang memungkinkan terjadinya pelanggaran data dan kerugian yang lebih besar, serta memengaruhi kepercayaan masyarakat terhadap keamanan informasi publik.

Ketiga, kurangnya kesadaran dan keterampilan di kalangan pegawai dan pengguna sistem dapat memperburuk situasi keamanan data secara signifikan. Tanpa pelatihan yang memadai dan pengetahuan yang cukup tentang praktik keamanan yang baik, pegawai mungkin tidak menyadari risiko atau cara-cara melindungi data dengan benar, sehingga meningkatkan kemungkinan terjadinya kesalahan manusia yang dapat menyebabkan pelanggaran keamanan. Meskipun pelatihan dilaksanakan, memastikan kepatuhan yang konsisten dari seluruh staf terhadap kebijakan keamanan tetap menjadi tantangan besar yang memerlukan pendekatan yang sistematis dan berkelanjutan untuk meningkatkan kesadaran dan disiplin dalam praktik keamanan.

Keempat, kompleksitas regulasi dan kepatuhan menjadi tantangan besar dalam menjaga keamanan data dan informasi, karena pemerintah harus memastikan bahwa kebijakan dan prosedur yang diterapkan sesuai dengan berbagai standar hukum dan regulasi, baik di tingkat nasional maupun internasional. Proses ini memerlukan perhatian yang teliti dan upaya berkelanjutan untuk mengikuti perkembangan regulasi yang sering kali berubah. Ketidakpatuhan terhadap regulasi ini tidak hanya dapat mengakibatkan sanksi hukum yang berat, tetapi juga dapat merusak kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data dan informasi, yang berpotensi menurunkan efektivitas transformasi digital yang diupayakan.

Kelima, integrasi dan interoperabilitas sistem yang berbeda dalam organisasi pemerintah menjadi kendala alinnya dalam menjaga keamanan data dan informasi. Sistem yang terpisah atau tidak kompatibel sering kali menyulitkan pengelolaan keamanan secara menyeluruh, karena data harus dikelola di berbagai platform dengan standar yang mungkin berbeda-beda. Hal ini dapat meningkatkan risiko kebocoran data atau pelanggaran keamanan, karena kurangnya koordinasi antar sistem dapat menciptakan celah keamanan yang dimanfaatkan oleh pihak tidak bertanggung jawab. Proses integrasi sistem yang efektif memerlukan desain arsitektur yang baik, pengembangan standar interoperabilitas, dan implementasi mekanisme keamanan yang konsisten di seluruh platform.

Secara konseptual, hambatan tersebut dapat dipahami melalui perspektif arsitektur sistem informasi yang menekankan pentingnya integrasi dan interoperabilitas. Dalam kerangka teori arsitektur TI, sistem yang terhubung perlu dirancang untuk memungkinkan pertukaran data yang aman dan efisien di antara berbagai komponen. Prinsip interoperabilitas dan standardisasi menggarisbawahi perlunya penerapan standar terbuka dan protokol yang seragam guna memastikan keselarasan fungsional sistem serta meminimalkan risiko keamanan (Hodapp, 2022). Dengan mengadopsi prinsip-prinsip tersebut, organisasi dapat memperkuat keamanan data melalui pengelolaan sistem yang lebih terstruktur serta mengurangi potensi kerentanan yang muncul akibat ketidakterpaduan antarplatform teknologi.

Untuk mengatasi tantangan dalam menjaga efektivitas keamanan data dan informasi, pemerintah perlu menerapkan beberapa rekomendasi berdasarkan teori dan praktik terbaik yang ada. Dalam menghadapi evolusi ancaman siber yang cepat, pemerintah harus mengadopsi pendekatan yang proaktif dengan menerapkan prinsip keamanan berlapis (defense-in-depth) dan memperbarui sistem secara berkala. Menurut teori manajemen risiko, pendekatan ini melibatkan penggunaan berbagai lapisan proteksi yang saling melengkapi, seperti firewall, sistem deteksi intrusi, dan perangkat lunak antivirus terbaru. Dengan cara ini, jika satu lapisan proteksi gagal, lapisan lainnya masih dapat mencegah serangan. Selain itu, pembaruan dan patching sistem yang rutin sangat penting untuk melindungi dari kerentanan yang baru ditemukan dan memastikan bahwa sistem tetap efektif melawan ancaman yang berkembang.

Selanjutnya, untuk mengatasi keterbatasan anggaran dan sumber daya, pemerintah dapat menerapkan model manajemen anggaran yang berbasis risiko, yang menekankan prioritas pada area yang paling rentan dan kritis. Teori pengelolaan anggaran berbasis risiko menyarankan alokasi sumber daya yang lebih efisien dengan fokus pada investasi di area yang memberikan dampak terbesar terhadap keamanan. Ini termasuk memilih solusi keamanan yang skalabel dan mengoptimalkan penggunaan sumber daya melalui kemitraan dengan penyedia teknologi dan pelatihan. Pemerintah juga dapat memanfaatkan inisiatif dan hibah dari lembaga internasional atau sektor swasta yang mendukung pengembangan kapasitas keamanan siber. Dengan pendekatan ini, pemerintah dapat mengatasi keterbatasan anggaran dengan lebih efektif dan memastikan bahwa sistem keamanan tetap terjaga dengan baik.

Pelajaran bagi pemerintah Kota Makassar dalam upaya menjaga efektifitas keamanan data dan informasi berdasarkan hasil penelitian global

Berdasarkan data global *Cost of a Data Breach Report 2025*, kerugian ekonomi rata-rata akibat kebocoran data mencapai **USD 4,44 juta per insiden** pada 2025, mencerminkan peningkatan risiko keamanan yang signifikan di seluruh sektor (IBM, 2025). Dengan tingginya biaya dan kompleksitas insiden siber ini, pemerintah Kota Makassar dapat belajar bahwa langkah proaktif seperti adopsi pendekatan berbasis risiko, kolaborasi antar sektor, pelatihan pegawai, serta penerapan standar keamanan internasional bukanlah pilihan opsional, melainkan kebutuhan mendesak untuk menjaga efektivitas keamanan data dan informasi dalam percepatan transformasi digital kota.

Menarik pelajaran dari penelitian global mengenai keamanan data dan informasi sangat penting bagi pemerintah Kota Makassar, mengingat tantangan yang terus berkembang dalam lanskap keamanan siber. Dengan memahami praktik dan strategi yang telah diterapkan di berbagai belahan dunia, pemerintah Kota Makassar dapat mengidentifikasi pendekatan yang efektif dan menyesuaikan langkah-langkah mereka untuk mengatasi tantangan lokal secara lebih baik. Pembelajaran dari pengalaman global tidak hanya memberikan panduan tentang cara memperbaiki kebijakan dan prosedur keamanan yang ada tetapi juga membantu dalam merumuskan strategi proaktif untuk melindungi data dan informasi publik di era digital. Hal ini mendukung upaya pemerintah dalam memastikan keamanan data yang lebih baik, meningkatkan kepercayaan publik, dan mengoptimalkan proses transformasi digital di tingkat kota.

Berdasarkan hasil penelitian global, beberapa pelajaran penting dapat diambil untuk memperkuat efektivitas keamanan data dan informasi di Kota Makassar. Pertama, pentingnya adopsi pendekatan berbasis risiko dalam keamanan siber (Hoffmann, Napiórkowski, Protasowicki, & Stanik, 2020). Penelitian internasional menunjukkan bahwa pendekatan ini memungkinkan organisasi untuk fokus pada ancaman yang paling signifikan dan mengalokasikan sumber daya secara lebih efisien. Dengan melakukan penilaian risiko secara teratur, pemerintah Kota Makassar dapat mengidentifikasi area yang paling rentan dan menerapkan langkah-langkah perlindungan yang sesuai, daripada mencoba mengatasi semua potensi ancaman secara bersamaan. Pendekatan berbasis risiko juga membantu dalam prioritisasi tindakan keamanan, yang sangat penting ketika anggaran dan sumber daya terbatas.

Kedua, kolaborasi dan berbagi informasi antara organisasi pemerintah dan sektor swasta merupakan praktik yang terbukti efektif dalam meningkatkan keamanan data. Penelitian global menunjukkan bahwa kemitraan ini memungkinkan akses ke intelijen ancaman yang lebih baik, serta teknik dan alat terbaru untuk menghadapi ancaman siber (Farrand & Carrapico, 2022). Untuk Kota Makassar, membangun jaringan kolaboratif dengan berbagai pemangku kepentingan—termasuk lembaga pemerintah lain, penyedia layanan teknologi, dan sektor industri—dapat memperkuat pertahanan siber secara keseluruhan. Melalui kolaborasi ini, Kota Makassar dapat memanfaatkan pengetahuan dan sumber daya yang lebih luas, serta memperbaiki respons terhadap insiden dengan lebih cepat.

Ketiga, pentingnya pelatihan dan pengembangan berkelanjutan untuk pegawai. Studi internasional menunjukkan bahwa program pelatihan yang berkelanjutan dan adaptif terhadap perubahan ancaman siber dapat mengurangi kesalahan manusia dan meningkatkan kesadaran keamanan. Kota Makassar harus memastikan bahwa seluruh pegawai menerima pelatihan rutin dan memahami praktik terbaik dalam menjaga keamanan data. Pelatihan ini harus mencakup cara mengenali ancaman siber, penggunaan alat keamanan yang tepat, dan prosedur tanggap darurat untuk menangani insiden. Investasi dalam pelatihan berkelanjutan akan memperkuat lapisan perlindungan manusia, yang sering kali menjadi garis pertahanan pertama terhadap serangan siber.

Keempat, penerapan kebijakan dan standar internasional dalam keamanan data juga menjadi pelajaran penting. Penelitian global menunjukkan bahwa mengikuti standar seperti General Data Protection

Regulation (GDPR) di Eropa (Padden & Öjehag-Pettersson, 2021), atau standar keamanan siber dari NIST (National Institute of Standards and Technology) dapat meningkatkan kepatuhan dan keamanan data (Link, 2019). Kota Makassar dapat mengadopsi standar internasional ini sebagai panduan dalam menyusun kebijakan dan prosedur keamanan data, memastikan bahwa praktik mereka sejalan dengan praktik terbaik global. Hal ini tidak hanya membantu dalam mematuhi regulasi yang berlaku tetapi juga dalam membangun kepercayaan publik terhadap kemampuan pemerintah dalam melindungi informasi.

Implikasi bagi pemerintah Kota Makassar adalah penerapan pelajaran dari penelitian global akan memperkuat kemampuan mereka dalam menghadapi ancaman siber yang semakin kompleks dan dinamis. Dengan mengintegrasikan praktik terbaik internasional ke dalam kebijakan dan prosedur lokal, pemerintah dapat meningkatkan keamanan data dan informasi secara keseluruhan, memastikan kepatuhan terhadap standar global, dan membangun kepercayaan publik. Hal ini akan mendukung transformasi digital dengan menciptakan lingkungan yang lebih aman dan stabil, memitigasi risiko, dan meningkatkan efisiensi operasional. Dengan demikian, Kota Makassar tidak hanya akan melindungi aset digitalnya secara lebih efektif tetapi juga akan mendorong kemajuan digital yang berkelanjutan, yang pada gilirannya dapat memperbaiki pelayanan publik dan meningkatkan kualitas hidup masyarakat.

PENUTUP

Upaya pemerintah Kota Makassar dalam meningkatkan efektivitas keamanan data dan informasi melibatkan langkah-langkah strategis yang sistematis dan komprehensif, sekaligus menghadapi berbagai tantangan yang muncul di era transformasi digital. Pemerintah telah melakukan penguatan infrastruktur keamanan melalui penggunaan firewall, enkripsi, dan sistem deteksi intrusi untuk menjaga kerahasiaan dan integritas data, disertai pelatihan teknis bagi pegawai untuk meminimalkan kesalahan manusia sebagai salah satu sumber kerentanan terbesar dalam keamanan siber. Selain itu, sosialisasi publik dilakukan untuk meningkatkan literasi keamanan digital sesuai dengan prinsip kesadaran risiko, serta monitoring dan evaluasi berkala diterapkan untuk memastikan adaptasi berkelanjutan terhadap ancaman baru. Namun, efektivitas upaya tersebut masih dipengaruhi oleh sejumlah tantangan utama, termasuk meningkatnya pola serangan siber yang semakin canggih, keterbatasan anggaran dan sumber daya teknologi, rendahnya kompetensi keamanan digital pegawai, kompleksitas regulasi yang memerlukan kepatuhan ketat, serta masalah integrasi dan interoperabilitas antar sistem yang berpotensi membuka celah serangan. Untuk menjawab tantangan tersebut, pemerintah perlu memperkuat penerapan keamanan berlapis dan pembaruan sistem secara rutin, mengelola anggaran dengan pendekatan berbasis risiko serta memperluas kemitraan dengan sektor swasta, meningkatkan pelatihan berkelanjutan bagi pegawai, dan menyusun arsitektur sistem informasi yang terintegrasi untuk meminimalkan kerentanan teknis.

DAFTAR PUSTAKA

Aldifansa, R., Wicaksono, N. D., Nurfadilah, A. H., Santoso Gunawan, A. A., & Edbert, I. S. (2023). Surveying the Impact of National Identity Card Data Leak to the Security and Serenity in Indonesia. *Proceeding - International Conference on Information Technology and Computing 2023, ICITCOM 2023*, 12–16. https://doi.org/10.1109/ICITCOM60176.2023.10442727

Alharbi, A. S., Halikias, G., Rajarajan, M., & Yamin, M. (2021). A review of effectiveness of Saudi E-government data security management. *International Journal of Information Technology (Singapore)*, *13*(2), 573–579. https://doi.org/10.1007/s41870-021-00611-3

Arunprasath, S., & Annamalai, S. (2024). Improving patient centric data retrieval and cyber security in healthcare: privacy preserving solutions for a secure future. *Multimedia Tools and Applications*, 18253. https://doi.org/10.1007/s11042-024-18253-5

Baharuddin, T. (2020). Keterbukaan Informasi Publik: Studi Pada Keberhasilan Pemerintah Daerah Kabupaten Luwu Utara 2019. *Journal of Governance and Local Politics*, *2*(2), 151–163. https://doi.org/10.47650/jglp.v2i2.133

Chadwick, D. W., Fan, W., Costantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., … Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, *102*, 710–722. https://doi.org/10.1016/j.future.2019.06.026

Chen, X., Tang, X., & Xu, X. (2023). Digital technology-driven smart society governance mechanism and practice exploration. *Frontiers of Engineering Management*, *10*(2), 319–338. https://doi.org/10.1007/s42524-022-0200-x

Chen, Y., kumara, E. K., & Sivakumar, V. (2023). RETRACTED ARTICLE: Investigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research*, *326*(s1), 15. https://doi.org/10.1007/s10479-021-04287-7

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*(June), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Fatir, M. D. (2019, April 2). Dinas Kominfo Makassar libatkan Badan Siber dan Sandi Negara. *Antaranews.Com*. Retrieved from https://makassar.antaranews.com/berita/117769/dinas-kominfo-makassar-libatkan-badan-siber-dan-sandi-negara

Fisdian Adni, D., Rusadi, S., & Baharuddin, T. (2024). Adaptive Policy in Website-Based Digitization of

Government Public Services: A Thematic Analysis. *Journal of Local Government Issues*, *7*(1), 54–67. https://doi.org/10.22219/logos.v7i1.29404

Golightly, L., Wnuk, K., Shanmugan, N., Shaban, A., Longstaff, J., & Chang, V. (2022). Towards a Working Conceptual Framework: Cyber Law for Data Privacy and Information Security Management for the Industrial Internet of Things Application Domain. *Proceedings - 2022 International Conference on Industrial IoT, Big Data and Supply Chain, IIoTBDSC 2022*, 86–94. https://doi.org/10.1109/IIoTBDSC57192.2022.00027

Haghighi, M. S., Farivar, F., Jolfaei, A., Asl, A. B., & Zhou, W. (2023). Cyber Attacks via Consumer Electronics: Studying the Threat of Covert Malware in Smart and Autonomous Vehicles. *IEEE Transactions on Consumer Electronics*, 3297965. https://doi.org/10.1109/TCE.2023.3297965

Hodapp, D. (2022). Interoperability in the era of digital innovation : An information systems research agenda. *Journal of Information Technology*, *0*(0), 1–21. https://doi.org/10.1177/02683962211064304

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, *44*(2019), 655–662. https://doi.org/10.1016/j.promfg.2020.02.243

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

IBM. (2025). *Cost of a Data Breach*. Retrieved from https://www.ibm.com/reports/data-breach

Ibrahim, A. H. H., Baharuddin, T., & Wance, M. (2023). Bibliometric Analysis of E-Government and Trust : A Lesson for Indonesia. *Jurnal Borneo Administrator*, *19*(3), 269–284. https://doi.org/10.24258/jba.v19i3.1303

Isabella, Agustian, E., Baharuddin, T., & Ibrahim, A. H. H. (2025). Bridging E-Government With Digital Literacy: a Literature Review. *Journal of Governance and Regulation*, *14*(1 (special issue)), 361–371. https://doi.org/10.22495/jgrv14i1siart12

Isabella, Alfitri, Saptawan, A., Nengyanti, & Baharuddin, T. (2024). Empowering Digital Citizenship in Indonesia : Navigating Urgent Digital Literacy Challenges for Effective Digital Governance. *Journal of Governance and Public Policy*, *11*(2), 142–155. https://doi.org/https://doi.org/10.18196/jgpp.v11i2.19258

Kang, H., & Deng, J. (2023). A cross encryption scheme for data security storage in cloud computing environment. *International Journal of Internet Protocol Technology*, *16*(1), 1–10. https://doi.org/10.1504/IJIPT.2023.129745

Kristensen, K., & Andersen, K. N. (2023). C-suite Leadership of Digital Government. *Digital Government: Research and Practice*, *4*(1), 3580000. https://doi.org/10.1145/3580000

Link, A. N. (2019). Technology transfer at the US National Institute of Standards and Technology. *Science*

and Public Policy, *46*(6), 906–912. https://doi.org/10.1093/scipol/scz038

Mohd, N., & Yunos, Z. (2020). Mitigating insider threats: A case study of data leak prevention. *European Conference on Information Warfare and Security, ECCWS*, *2020-June*, 599–605. https://doi.org/10.34190/EWS.20.004

Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies*, *15*(4), 486–503. https://doi.org/10.1080/19460171.2021.1927776

Pham, T. H., Phan, T. A., Trinh, P. A., Mai, X. B., & Le, Q. C. (2023). Information security risks and sharing behavior on OSN: the impact of data collection awareness. *Journal of Information, Communication and Ethics in Society*, 2024. https://doi.org/10.1108/JICES-06-2023-0076

Ren, S., Chen, D., Tao, Y., Xu, S., Wang, G., & Yang, Z. (2022). Intelligent terminal security technology of power grid sensing layer based upon information entropy data mining. *Journal of Intelligent Systems*, *31*(1), 817–834. https://doi.org/10.1515/jisys-2022-0117

Salahudin, S., Nurmandi, A., & Loilatu, M. J. (2020). How to Design Qualitative Research with NVivo 12 Plus for Local Government Corruption Issues in Indonesia? *Jurnal Studi Pemerintahan*, *11*(3), 369–398. https://doi.org/10.18196/jgp.113124

Sarkar, S., & Das, S. (2022). Fuzzy based security risk assessment of e-government data centre in Indian context. *Electronic Government*, *18*(3), 354–380. https://doi.org/10.1504/EG.2022.123838

Scupola, A., & Mergel, I. (2022). Co-production in digital transformation of public administration and public value creation: The case of Denmark. *Government Information Quarterly*, *39*(1), 101650. https://doi.org/10.1016/j.giq.2021.101650

Sharma, R., Fantin, A. R., Prabhu, N., Guan, C., & Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. *Telecommunications Policy*, *40*(7), 628–643. https://doi.org/10.1016/j.telpol.2016.05.003

Sharma, S., Rahaman, V., & Sinha, G. R. (2021). Big Data Analytics in Cognitive Social Media and Literary Texts: Theory and Praxis. *Big Data Analytics in Cognitive Social Media and Literary Texts: Theory and Praxis*, 1–300. https://doi.org/10.1007/978-981-16-4729-1

Vrhovec, S., & Markelj, B. (2018). Relating mobile device use and adherence to information security policy with data breach consequences in hospitals. *Journal of Universal Computer Science*, *24*(5), 634–645.

Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*, 104771. https://doi.org/10.1016/j.scs.2023.104771

Yuan, Y. P., Dwivedi, Y. K., Tan, G. W. H., Cham, T. H., Ooi, K. B., Aw, E. C. X., & Currie, W. (2023). Government Digital Transformation: Understanding the Role of Government Social Media. *Government Information Quarterly*, *40*(1), 101775. https://doi.org/10.1016/j.giq.2022.101775