JURNAL SINTAKS LOGIKA Vol. 6 No. 2, Mei 2026 , pp. 141-152, **eISSN : 2775-412X**
https://jurnal.umpar.ac.id/index.php/sylog

Perlindungan Data dan Privasi dalam Perspektif Islam

Afiqah Nur Syafitri HS[1*], Elsa Yakub[2], Resky Amelia[3], Elisa Emi putri[4], Euneng Mutiara Munanda[5], Rabiatul Adawiyah Fair[6], Reski Amalia[7], Miftah Khaeria[8], Besse Ruhaya[9]

[1*,2,3,4,5,6,7,8,9]*Program Studi Teknik Informatika, Universitas Islam Negeri Alauddin Makassar, Indonesia*

*Email : afiqahnur2910@gmail.com

Abstract: The rapid advancement of digital technology has increased the collection and processing of personal data while also intensifying the risk of data breaches and privacy violations. This study aims to analyze personal data protection from the perspective of Islamic law and *maqashid al-shariah* and examine its integration with information security technologies and data protection regulations. This research employed a qualitative method using a library research approach through the analysis of the Qur'an, Hadith, scientific books, journal articles, and relevant legislation. The results show that Islamic values, including *amanah*, the prohibition of *tajassus*, and the principles of *maqashid al-shariah*, provide a strong ethical foundation for protecting personal data. These principles are consistent with Indonesia's Personal Data Protection Law and can be implemented through information security technologies such as encryption, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Zero Trust Architecture, Artificial Intelligence, Security by Design, and Privacy by Design. This study proposes an integrated conceptual model that combines Islamic ethical values, legal compliance, and information security technologies to support secure, accountable, and sustainable personal data governance in the digital era.

Keywords: personal_data; privacy; maqashid_al-shariah; information_security; zero_trust

1. PENDAHULUAN

Transformasi digital telah mendorong pemanfaatan teknologi seperti *Big Data*, *Cloud Computing*, *Internet of Things* (IoT), dan *Artificial Intelligence* (AI) dalam berbagai sektor. Perkembangan tersebut meningkatkan efisiensi pengelolaan data sekaligus memperluas penggunaan data pribadi dalam layanan digital. Di sisi lain, meningkatnya aktivitas digital juga diikuti oleh berbagai ancaman keamanan, seperti kebocoran data, pencurian identitas, penyalahgunaan informasi pribadi, dan serangan siber. Kondisi ini menjadikan perlindungan data pribadi sebagai salah satu aspek penting dalam mewujudkan keamanan informasi dan menjaga hak privasi pengguna (Tsouplaki et al., 2025).

Sebagai upaya memberikan kepastian hukum, pemerintah Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, keberadaan regulasi saja belum cukup untuk menjamin keamanan data apabila tidak didukung oleh penerapan teknologi keamanan informasi dan kesadaran etis dalam pengelolaan data. Oleh karena itu, diperlukan pendekatan yang mampu

mengintegrasikan aspek hukum, teknologi, dan nilai-nilai moral dalam perlindungan data pribadi.

Beberapa penelitian terdahulu telah mengkaji perlindungan data pribadi dari berbagai perspektif. (Putri, 2026) membahas perlindungan data dalam perspektif Islam, (Tirmidzi, 2025) mengkaji perlindungan data berdasarkan hukum pidana Islam, sedangkan (Thoriquttyas & Rohmawati, 2026) menjelaskan konsep *maqashid al-shariah* dalam kepemilikan data digital. Di sisi lain, (Tsouplaki et al., 2025) menyoroti pemanfaatan *Artificial Intelligence* dalam meningkatkan privasi pada lingkungan *Internet of Things*. Meskipun demikian, penelitian-penelitian tersebut masih membahas aspek hukum, etika Islam, atau teknologi secara terpisah sehingga belum memberikan kerangka yang mengintegrasikan ketiganya.

Berdasarkan kajian tersebut, masih terdapat kesenjangan penelitian (*research gap*) berupa belum adanya model konseptual yang mengintegrasikan nilai-nilai Islam, regulasi perlindungan data, dan teknologi keamanan informasi sebagai satu kesatuan dalam perlindungan data pribadi. Padahal, integrasi ketiga aspek tersebut diperlukan untuk mewujudkan tata kelola data yang aman, bertanggung jawab, dan berkelanjutan.

Penelitian ini menggunakan pendekatan *library research* untuk menganalisis konsep perlindungan data pribadi dari perspektif Islam, regulasi perlindungan data, dan teknologi keamanan informasi. Kebaruan (novelty) penelitian ini terletak pada pengembangan model integrasi yang menggabungkan nilai-nilai *maqashid al-shariah*, regulasi perlindungan data, dan teknologi keamanan informasi sebagai kerangka konseptual dalam mendukung perlindungan data pribadi di era transformasi digital.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan *library research* (studi kepustakaan). Data penelitian diperoleh dari berbagai sumber yang relevan, meliputi Al-Qur'an, Hadis, buku ilmiah, artikel jurnal nasional dan internasional, serta peraturan perundang-undangan, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Literatur dipilih berdasarkan relevansi dengan topik perlindungan data pribadi, *maqashid al-shariah*, dan teknologi keamanan informasi.

Prosedur penelitian meliputi identifikasi dan pengumpulan literatur, seleksi sumber berdasarkan kesesuaian dengan tujuan penelitian, klasifikasi literatur ke dalam aspek nilai-nilai Islam, regulasi, dan teknologi keamanan informasi, kemudian dilakukan analisis secara deskriptif-kualitatif. Hasil analisis selanjutnya disintesis untuk merumuskan model integrasi perlindungan data pribadi yang menggabungkan nilai-nilai Islam, regulasi perlindungan data, dan teknologi keamanan informasi sebagai kerangka konseptual dalam mendukung tata kelola data yang aman dan bertanggung jawab di era transformasi digital.

3. HASIL DAN PEMBAHASAN

3.1. Perlindungan Data Pribadi pada Era Transformasi Digital

Transformasi digital telah mengubah cara individu, organisasi, dan pemerintah mengelola informasi melalui pemanfaatan *Big Data*, *Cloud Computing*, *Internet of Things*

(IoT), dan *Artificial Intelligence* (AI). Teknologi tersebut memungkinkan pengolahan data secara lebih cepat dan efisien sehingga meningkatkan kualitas layanan di berbagai sektor. Namun, meningkatnya konektivitas digital juga memperluas attack surface yang berdampak pada meningkatnya risiko kebocoran data, pencurian identitas, serta penyalahgunaan informasi pribadi. Kondisi ini menunjukkan bahwa perlindungan data telah menjadi bagian penting dari tata kelola keamanan informasi (Marengo, 2024).

Perkembangan *Big Data* dan *Cloud Computing* memungkinkan organisasi mengelola data dalam jumlah besar untuk mendukung pengambilan keputusan. Di sisi lain, semakin besar volume data yang diproses, semakin tinggi pula risiko pelanggaran privasi apabila tidak didukung oleh mekanisme keamanan yang memadai. Penelitian menunjukkan bahwa penerapan enkripsi, anonimisasi, differential privacy, serta pengendalian akses merupakan langkah penting dalam menjaga kerahasiaan dan keamanan data (Almosti & Rahman, 2025; Rafiq et al., 2022).

Menurut analisis penulis, keberhasilan transformasi digital tidak hanya ditentukan oleh kemampuan organisasi mengadopsi teknologi, tetapi juga oleh kemampuannya membangun sistem keamanan informasi yang terintegrasi. Perlindungan data seharusnya menjadi bagian dari perancangan sistem sejak awal (*security by design*), sehingga keamanan tidak hanya diterapkan ketika terjadi insiden, tetapi menjadi karakteristik utama dari sistem yang dikembangkan.

Perkembangan IoT dan AI semakin memperkuat kebutuhan terhadap perlindungan data karena perangkat yang saling terhubung menghasilkan informasi dalam jumlah besar dan bersifat sensitif. AI mampu mendeteksi anomali, mengidentifikasi pola serangan siber, serta meningkatkan respons keamanan secara real-time. Namun, penggunaan AI juga memerlukan pendekatan privacy-preserving, seperti federated learning dan differential privacy, agar pemanfaatan data tetap menghormati hak privasi pengguna (Alzoubi & Mishra, 2025; Kaur et al., 2025; Tsouplaki et al., 2025).

Berdasarkan analisis penelitian ini, perlindungan data pribadi harus dipandang sebagai fondasi utama dalam transformasi digital. Integrasi teknologi keamanan informasi, tata kelola data yang baik, dan penerapan prinsip *security by design* serta *privacy by design* akan menghasilkan sistem yang lebih aman, meningkatkan kepercayaan pengguna, dan mendukung keberlanjutan layanan digital.

3.2. Perlindungan Data dalam Perspektif Maqashid Syariah

Transformasi digital telah menjadikan data pribadi sebagai aset yang memiliki nilai ekonomi, sosial, dan hukum. Dalam perspektif Islam, perlindungan data pribadi tidak hanya merupakan kewajiban hukum, tetapi juga bagian dari tanggung jawab moral untuk menjaga hak dan martabat manusia. Maqashid syariah memberikan landasan etis yang relevan karena bertujuan mewujudkan kemaslahatan (*maslahah*) dan mencegah kerusakan (*mafsadah*). Penelitian menunjukkan bahwa konsep ini dapat menjadi dasar dalam membangun tata kelola data yang adil dan bertanggung jawab di era digital (Arminsyah, 2025; Thoriquttyas & Rohmawati, 2026).

Salah satu prinsip utama adalah amanah, yaitu kewajiban menjaga kepercayaan dalam mengelola data pribadi. Dalam sistem informasi, amanah mengharuskan

pengelola data memproses informasi hanya sesuai tujuan yang telah disepakati dan melindunginya dari penyalahgunaan (Putra et al., 2024). Menurut analisis penelitian ini, prinsip tersebut dapat diwujudkan melalui penerapan teknologi keamanan seperti enkripsi, Multi-Factor Authentication (MFA), dan Role-Based Access Control (RBAC) sehingga pengelolaan data tidak hanya memenuhi aspek teknis, tetapi juga mencerminkan tanggung jawab etis.

Islam juga melarang tajassus, yaitu mengakses informasi pribadi tanpa hak, sebagaimana ditegaskan dalam QS. Al-Hujurat ayat 12. Prinsip ini sejalan dengan perlindungan privasi digital terhadap praktik seperti pengumpulan data tanpa persetujuan, penyadapan, maupun penyalahgunaan informasi pribadi. Kajian terbaru menegaskan bahwa hak atas privasi merupakan bagian dari ḥifẓ al-'irḍ (menjaga kehormatan), sehingga perlu dilindungi melalui regulasi dan teknologi keamanan informasi (Nidhom & Murtadho, 2025).

Selain itu, ḥifẓ al-'irḍ, ḥifẓ al-māl, dan ḥifẓ an-nafs memiliki relevansi dalam perlindungan data digital. Identitas digital perlu dijaga dari pencurian identitas dan penyalahgunaan informasi, sementara data pribadi juga memiliki nilai ekonomi yang harus dilindungi dari penipuan maupun kejahatan siber (Arminsyah, 2025; Thoriquttyas & Rohmawati, 2026). Di sisi lain, kebocoran data kesehatan, lokasi, atau informasi sensitif lainnya dapat mengancam keselamatan dan kesejahteraan individu (Putra et al., 2024). Menurut analisis penulis, penerapan teknologi keamanan informasi merupakan bentuk implementasi maqashid syariah dalam menjaga kehormatan, harta, dan keselamatan manusia di ruang digital.

Berdasarkan pembahasan tersebut, maqashid syariah tidak bertentangan dengan perkembangan teknologi, tetapi justru menjadi landasan etis yang memperkuat implementasi teknologi perlindungan data. Integrasi nilai Islam dengan regulasi dan teknologi keamanan informasi memungkinkan terciptanya tata kelola data yang aman, bertanggung jawab, dan berorientasi pada kemaslahatan masyarakat.

3.3. Implementasi Teknologi Perlindungan Data Pribadi

3.3.1 Teknologi Keamanan Data

Perlindungan data pribadi dalam sistem informasi memerlukan penerapan berbagai teknologi keamanan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data. Teknologi seperti enkripsi (*encryption*), hashing, dan tokenization digunakan untuk melindungi data sensitif, sedangkan firewall, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), dan Virtual Private Network (VPN) berfungsi mengamankan jaringan dari akses maupun serangan yang tidak sah. Selain itu, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), dan Security Information and Event Management (SIEM) diterapkan untuk mengendalikan hak akses, memperkuat autentikasi, serta memantau aktivitas keamanan secara terpusat (Akbar Prasetyo & Chalik Azhar, 2025; Arits Fikri et al., 2026; Huda & Subektiningsih, 2024).

Berdasarkan analisis penelitian ini, efektivitas perlindungan data tidak ditentukan oleh satu teknologi, tetapi oleh integrasi berbagai mekanisme keamanan yang saling

melengkapi. Enkripsi melindungi kerahasiaan data, sedangkan RBAC dan MFA memastikan bahwa hanya pengguna yang berwenang dapat mengakses informasi. Di sisi lain, firewall, IDS/IPS, dan SIEM berperan dalam mendeteksi serta merespons ancaman siber secara lebih cepat. Menurut penulis, pendekatan defense in depth lebih efektif karena menyediakan beberapa lapisan perlindungan sehingga apabila satu mekanisme mengalami kelemahan, lapisan keamanan lainnya tetap mampu meminimalkan risiko kebocoran data.

Selain penerapan teknologi, organisasi juga perlu mengintegrasikan prinsip Security by Design sejak tahap perancangan sistem. Menurut analisis penulis, pendekatan ini memungkinkan keamanan menjadi bagian dari arsitektur sistem, bukan hanya fitur tambahan setelah sistem dioperasikan. Dengan demikian, teknologi keamanan tidak hanya melindungi data dari ancaman siber, tetapi juga mendukung kepatuhan terhadap regulasi perlindungan data serta meningkatkan kepercayaan pengguna terhadap layanan digital.

3.3.2 Proses Perlindungan Data

Perlindungan data pribadi merupakan proses berkelanjutan sepanjang siklus hidup data (*data life cycle*) untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Berdasarkan praktik keamanan modern, proses ini mencakup pengumpulan, persetujuan (*consent*), validasi, enkripsi, penyimpanan, pengendalian akses, pemantauan (*monitoring*), *audit log*, *backup*, *recovery*, serta penghapusan atau anonimisasi data. Penerapan menyeluruh ini mengintegrasikan prinsip *Privacy by Design* dan *Security by Design* sejak data pertama kali diperoleh hingga tidak lagi digunakan (Arits Fikri et al., 2026; Fauzi et al., 2025).

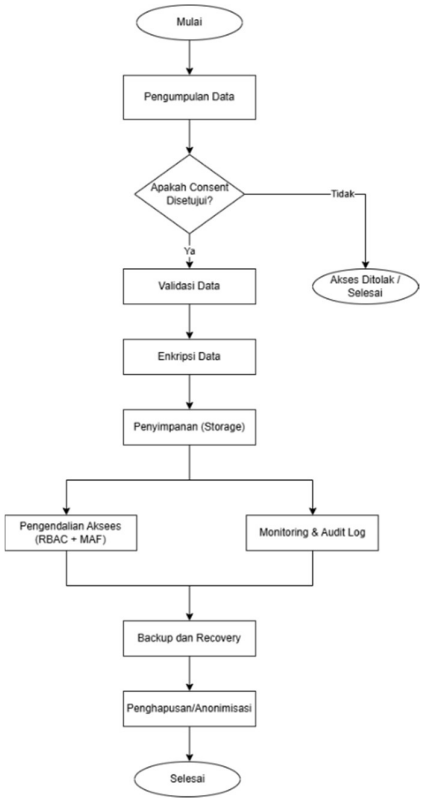
Berdasarkan analisis penelitian ini, alur dimulai pada tahap pengumpulan data dengan prinsip *data minimization*, yaitu membatasi input hanya pada data yang benar-benar diperlukan. Selanjutnya, sistem melakukan pemeriksaan *consent* secara transparan. Jika pengguna menolak (*consent* ditolak), alur sistem langsung berhenti (*terminate*) dan akses layanan ditolak. Sebaliknya, jika disetujui, alur berlanjut ke tahap validasi data untuk memastikan akurasi, kelengkapan, dan relevansi informasi sebelum diproses lebih lanjut guna menghindari risiko penyalahgunaan.

Setelah divalidasi, data wajib diamankan melalui enkripsi terlebih dahulu sebelum disimpan ke dalam media penyimpanan (*storage*). Begitu data menetap di basis data, pengendalian akses ketat diterapkan menggunakan kombinasi *Role-Based Access Control* (RBAC) dan *Multi-Factor Authentication* (MFA). Secara simultan, seluruh aktivitas di dalam sistem dicatat melalui *audit log* dan diawasi oleh sistem *monitoring*. Menurut analisis penulis, sinergi antara pembatasan akses (RBAC + MFA) dan pengawasan *real-time* ini sangat krusial untuk mendeteksi anomali serta mencegah kebocoran data baik dari ancaman internal maupun eksternal.

Tahap berikutnya adalah prosedur *backup* dan *recovery* yang berjalan secara paralel di latar belakang untuk menjamin ketersediaan (*availability*) data. Mekanisme pemulihan (*recovery*) siap diaktifkan jika terjadi kegagalan sistem atau serangan *ransomware* guna meminimalkan waktu henti (*downtime*) operasional. Siklus hidup data berakhir ketika masa retensi habis atau data tidak lagi dibutuhkan, di mana organisasi

wajib melakukan penghapusan aman (*secure deletion*) atau anonimisasi. Menurut analisis penelitian ini, pemusnahan data yang aman sangat penting untuk mencegah eksploitasi sisa-sisa data (*data remnants*) yang tertinggal di media penyimpanan.

Secara keseluruhan, alur ini membuktikan bahwa perlindungan data pribadi tidak dapat bertumpu pada satu teknologi tunggal, melainkan pada penerapan keamanan berlapis di setiap tahapan pengelolaan data. Pendekatan terintegrasi ini efektif membantu organisasi memenuhi kepatuhan regulasi sekaligus meningkatkan kepercayaan pengguna terhadap layanan digital.



Gambar 3. Alur proses perlindungan data pribadi pada sistem informasi.

3.3.3 Zero Trust Architecture

Seiring Meningkatnya ancaman siber dan kompleksitas sistem informasi mendorong organisasi beralih dari model keamanan tradisional menuju *Zero Trust Architecture* (ZTA). Pendekatan ini menerapkan prinsip "Never Trust, Always Verify", yaitu setiap pengguna, perangkat, maupun aplikasi harus melalui proses verifikasi sebelum memperoleh akses ke sumber daya sistem. Implementasi ZTA didukung oleh prinsip *Least Privilege Access*, *Continuous Authentication*, dan *Continuous Monitoring* untuk meminimalkan risiko akses tidak sah serta melindungi data pribadi dari berbagai ancaman siber (Daah et al., 2024; Durga, 2025)

Berdasarkan analisis penelitian ini, *Least Privilege Access* memastikan pengguna hanya memperoleh hak akses sesuai kewenangannya, sedangkan *Continuous Authentication* dan *Continuous Monitoring* memungkinkan sistem memverifikasi identitas

serta memantau aktivitas pengguna secara berkelanjutan. Menurut penulis, kombinasi ketiga prinsip tersebut mampu mengurangi risiko pencurian kredensial, penyalahgunaan akun, dan *lateral movement* karena setiap permintaan akses selalu dievaluasi berdasarkan identitas, kondisi perangkat, dan tingkat risiko yang terdeteksi. Selain itu, ZTA mengintegrasikan teknologi seperti MFA, RBAC, enkripsi, dan SIEM sehingga membentuk sistem keamanan yang lebih adaptif dan berlapis.

Dalam konteks Indonesia, penerapan *Zero Trust Architecture* sejalan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mewajibkan pengendali data menerapkan langkah teknis dan organisasi untuk melindungi data pribadi. Menurut analisis penulis, prinsip Never Trust, Always Verify mendukung kepatuhan terhadap UU PDP karena setiap akses terhadap data harus melalui autentikasi, otorisasi, dan pemantauan yang ketat. Dengan demikian, Zero Trust tidak hanya meningkatkan keamanan sistem informasi, tetapi juga memperkuat tata kelola data yang sesuai dengan regulasi dan kebutuhan organisasi modern.

3.3.4 Artificial Intelligence untuk Data Protection

Perkembangan *Artificial Intelligence* (AI) telah meningkatkan kemampuan sistem keamanan siber dalam melindungi data pribadi. AI mampu menganalisis data dalam jumlah besar untuk mendeteksi pola serangan, melakukan *User Behaviour Analytics* (UBA), mendeteksi *phishing*, *malware*, *fraud*, serta mendukung *predictive security* sehingga ancaman dapat diidentifikasi lebih cepat (Jamal et al., 2024; Okdem & Okdem, 2024)**.**

Berdasarkan analisis penelitian ini, AI memberikan keunggulan dalam meningkatkan kecepatan dan akurasi deteksi ancaman dibandingkan metode berbasis aturan (*rule-based system*). Pada User Behaviour Analytics, AI mampu mengenali aktivitas login yang tidak biasa, sedangkan pada deteksi phishing, malware, dan fraud, AI dapat mengidentifikasi pola serangan berdasarkan hasil pembelajaran dari data sebelumnya. Menurut penulis, kemampuan tersebut menjadikan AI sebagai teknologi yang mendukung predictive security, yaitu pendekatan keamanan yang mampu mendeteksi potensi serangan sebelum berdampak pada kebocoran data atau gangguan layanan.

Di sisi lain, penggunaan AI juga menghadapi tantangan etika, seperti risiko pelanggaran privasi, bias algoritma, kurangnya transparansi (*black box*), serta kemungkinan terjadinya false positive dan false negative. Menurut analisis penulis, AI sebaiknya berfungsi sebagai *decision support system*, bukan menggantikan pengambilan keputusan manusia. Oleh karena itu, penerapan AI perlu diintegrasikan dengan teknologi keamanan lain, seperti *Zero Trust Architecture*, Multi-Factor Authentication (MFA), dan Security Information and Event Management (SIEM), agar perlindungan data menjadi lebih adaptif, akurat, dan tetap sesuai dengan prinsip etika serta regulasi perlindungan data pribadi.

3.4. Integrasi Teknologi, Regulasi, dan Nilai Islam

3.4.1 Regulasi Perlindungan Data

Perlindungan data pribadi di Indonesia diperkuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi atas pelanggaran perlindungan data. Selain itu, Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas UU Informasi dan Transaksi Elektronik (UU ITE) memberikan dasar hukum bagi penyelenggaraan sistem elektronik dan perlindungan informasi digital. Kehadiran kedua regulasi tersebut menunjukkan bahwa perlindungan data merupakan tanggung jawab hukum sekaligus bagian dari tata kelola sistem informasi yang aman (Abita et al., 2024; Firdaus, 2024).

Berdasarkan analisis penelitian ini, regulasi tidak akan efektif apabila tidak didukung oleh implementasi teknologi keamanan. Ketentuan dalam UU PDP perlu diwujudkan melalui penerapan enkripsi, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), audit log, serta monitoring secara berkelanjutan. Menurut penulis, integrasi antara regulasi dan teknologi memungkinkan organisasi tidak hanya memenuhi kewajiban hukum, tetapi juga meningkatkan keamanan data sepanjang siklus hidupnya.

Sebagai pembanding, General Data Protection Regulation (GDPR) di Uni Eropa menerapkan prinsip *privacy by design, privacy by default*, transparansi pemrosesan data, dan penguatan hak subjek data. Meskipun implementasinya berbeda, UU PDP memiliki tujuan yang sejalan dalam memberikan perlindungan terhadap data pribadi. Pengalaman penerapan GDPR dapat menjadi referensi bagi Indonesia untuk memperkuat tata kelola data melalui sinergi antara kebijakan, teknologi, dan peningkatan kesadaran keamanan informasi (Taufiq & Kenyo, 2025)

Menurut analisis penulis, efektivitas perlindungan data bergantung pada keseimbangan antara regulasi, kesiapan teknologi, dan budaya keamanan informasi. Organisasi yang hanya berorientasi pada kepatuhan administratif tetap berisiko mengalami kebocoran data apabila sistem keamanannya lemah. Oleh karena itu, regulasi dan teknologi harus diterapkan secara terpadu agar perlindungan data pribadi dapat berjalan secara efektif, akuntabel, dan berkelanjutan.

3.4.2 Etika Islam dalam Tata Kelola Data

Penerapan teknologi perlindungan data pribadi tidak hanya memerlukan dukungan regulasi dan mekanisme keamanan, tetapi juga landasan etika dalam pengelolaan data. Dalam perspektif Islam, prinsip **amanah** mengharuskan setiap individu maupun organisasi menjaga data pribadi sesuai tujuan yang telah disetujui oleh pemiliknya. Selain itu, **maqashid syariah**, khususnya **ḥifẓ al-'irḍ** (menjaga kehormatan), memberikan dasar etis untuk melindungi hak privasi dan martabat individu di era digital (Putra et al., 2024; Thoriquttyas & Rohmawati, 2026).

Berdasarkan analisis penelitian ini, tanggung jawab menjaga data tidak hanya berada pada pengguna, tetapi juga pada pengendali data (data controller) dan pengembang sistem (developer). Pengembang perlu menerapkan prinsip *Security by*

Design dan *Privacy by Design* sejak tahap perancangan sistem agar keamanan dan privasi menjadi bagian dari arsitektur aplikasi. Menurut penulis, keberhasilan perlindungan data tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh komitmen pengelola dalam membangun sistem yang aman, transparan, dan menghormati hak pengguna.

Etika juga menjadi aspek penting dalam pemanfaatan *Artificial Intelligence* (AI) untuk perlindungan data. Meskipun AI mampu meningkatkan deteksi ancaman siber, penggunaannya harus memperhatikan prinsip transparansi, akuntabilitas, keadilan (*fairness*), dan perlindungan privasi agar tidak menimbulkan bias maupun pelanggaran hak individu. Menurut analisis penulis, AI sebaiknya berfungsi sebagai pendukung pengambilan keputusan (*decision support system*) yang tetap berada di bawah pengawasan manusia sehingga hasilnya lebih akurat, bertanggung jawab, dan sesuai dengan nilai-nilai etika.

Secara keseluruhan, integrasi antara nilai Islam, regulasi, dan teknologi keamanan informasi mampu menghasilkan tata kelola data yang tidak hanya memenuhi standar teknis dan hukum, tetapi juga mencerminkan tanggung jawab moral terhadap pemilik data. Pendekatan ini menjadi fondasi penting dalam membangun kepercayaan pengguna terhadap layanan digital.

3.4.3 Model Integrasi Perlindungan Data

Berdasarkan pembahasan sebelumnya, penelitian ini mengusulkan model integrasi perlindungan data pribadi yang menggabungkan tiga komponen utama, yaitu nilai Islam (maqashid syariah), regulasi perlindungan data, dan teknologi keamanan informasi. Ketiga komponen tersebut saling melengkapi dalam membangun tata kelola data yang aman, bertanggung jawab, dan berorientasi pada perlindungan hak privasi pengguna (Putra et al., 2024)

Menurut analisis penelitian ini, maqashid syariah berfungsi sebagai landasan etika yang mendorong pengelolaan data secara bertanggung jawab melalui prinsip amanah, ḥifẓ al-'irḍ, dan ḥifẓ al-māl. Selanjutnya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi dasar hukum yang mengatur hak subjek data dan kewajiban pengendali data. Kedua aspek tersebut kemudian diimplementasikan melalui teknologi keamanan seperti enkripsi, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), *Zero Trust Architecture*, *Artificial Intelligence* (AI), serta monitoring dan audit log untuk melindungi data sepanjang siklus hidupnya.

Berdasarkan sintesis penulis, perlindungan data yang efektif hanya dapat dicapai apabila ketiga komponen tersebut diterapkan secara terpadu. Regulasi tanpa dukungan teknologi akan sulit menghadapi ancaman siber, sedangkan teknologi tanpa landasan etika berpotensi menimbulkan penyalahgunaan data. Oleh karena itu, integrasi antara nilai moral, kepatuhan hukum, dan teknologi keamanan menjadi faktor penting dalam membangun tata kelola data yang aman dan berkelanjutan.

Model yang diusulkan menempatkan maqashid syariah sebagai fondasi etika, UU PDP sebagai kerangka regulasi, dan teknologi keamanan informasi sebagai instrumen implementasi. Menurut penulis, model ini dapat menjadi kerangka konseptual bagi organisasi maupun pengembang sistem informasi dalam merancang perlindungan data

yang tidak hanya memenuhi aspek teknis dan hukum, tetapi juga mencerminkan tanggung jawab etis sehingga mampu meningkatkan kepercayaan pengguna terhadap layanan digital.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa perlindungan data pribadi dalam perspektif Islam memiliki landasan yang kuat melalui prinsip *amanah*, larangan *tajassus*, dan *maqashid al-shariah*, yang selaras dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Perlindungan data yang efektif memerlukan integrasi antara nilai-nilai Islam, regulasi, dan teknologi keamanan informasi seperti encryption, RBAC, MFA, *Zero Trust Architecture*, dan *Artificial Intelligence*. Model integrasi yang diusulkan diharapkan dapat menjadi kerangka konseptual dalam membangun tata kelola data yang aman, bertanggung jawab, dan berkelanjutan di era transformasi digital.

REFERENSI

Abita, C., Irwandi, & Amin, M. (2024). PERBANDINGAN PERLINDUNGAN DATA PRIBADI ANTARA UNDANG-UNDANG NOMOR 27 TAHUN 2022 DENGAN UNDANG-UNDANG NOMOR 1 TAHUN 2024. *Limbago: Journal of Constitutional Law*, *4*.

Akbar Prasetyo, M., & Chalik Azhar, N. (2025). EVALUATION OF TWO-FACTOR AUTHENTICATION METHOD IN IMPROVING AUTHENTICATION SECURITY ON SSL VPN (Case Study of PT. Kanmo Group). *Jurnal Riset Informatika*, *7*(3), 186–191. https://doi.org/10.34288/jri.v7i3.367

Almosti, A. M., & Rahman, M. M. H. (2025). Analysis of Data Privacy Breaches Using Deep Learning in Cloud Environments: A Review. In *Electronics (Switzerland)* (Vol. 14, Number 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics14132727

Alzoubi, Y. I., & Mishra, A. (2025). Differential privacy and artificial intelligence: potentials, challenges, and future avenues. In *Eurasip Journal on Information Security* (Vol. 2025, Number 1). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s13635-025-00203-9

Arits Fikri, M. N., Sarwako, N. L., Denrineksa Bimorogo, S., Lediwara, N., & Khamas Heikhmakhtiar, A. (2026). Digital archiving using AES-256 encryption and role-based access control to strengthen data security at Pusdatin. *Jurnal Mandiri IT*, *14*(3), 381–391. www.ejournal.isha.or.id/index.php/Mandiri

Arminsyah, A. (2025). Maqasid al-Shariah in Contemporary Legal Systems: An Analysis of Digital Rights and Privacy Protection. *Al-Qadha : Jurnal Hukum Islam Dan Perundang-Undangan*, *12*(2), 289–308. https://doi.org/10.32505/qadha.v12i2.11178

Auda, J. (2008). Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach. London: International Institute of Islamic Thought (IIIT).

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics (Switzerland)*, *13*(5). https://doi.org/10.3390/electronics13050865

Durga, R. K. (2025). Implementing Zero Trust Architecture: Principles, Models and Challenges. *International Journal of Scientific Research and Modern Technology*, 162. https://doi.org/10.38124/ijsrmt.v4i12.1050

Fauzi, A., Nur Aprilla, I., Fauziyyah, N., & Fazriyanti Bachtiar, N. (2025). Implementasi Multi-Faktor Authentication, Single Sign-on dan Role-Based Access Control dalam Keamanan Sistem Informasi (Studi Literature Review). *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *2*(1). https://doi.org/10.63217/fibonacci.v2i1.256

Firdaus, F. H. (2024). PERLINDUNGAN DAN KEPASTIAN HUKUM BAGI PENGENDALI DATA PRIBADI DI MASA DEPAN. *JURNAL MASALAH-MASALAH HUKUM*, *53*.

Huda, T. S., & Subektiningsih. (2024). Analisis Keamanan Jaringan Komputer Menggunakan Metode IDS dan IPS dengan Notifikasi Telegram. *Indonesian Journal of Computer Science Attribution*, *13*(1), 2024–1335.

Jamal, S., Wimmer, H., & Sarker, I. H. (2024). An improved transformer-based model for detecting phishing, spam and ham emails: A large language model approach. *SECURITY AND PRIVACY*, *7*(5). https://doi.org/10.1002/spy2.402

Kaur, R., Rodrigues, T., Kadir, N., & Kashef, R. (2025). A Survey on Privacy Preservation Techniques in IoT Systems. In *Sensors* (Vol. 25, Number 22). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s25226967

Knibbs, C., & Hibberd, G. (Eds.). (2024). A practitioner's guide to cybersecurity and data protection: How to ensure client confidentiality. London: Routledge.

Marengo, A. (2024). Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms. In *Internet of Things (Netherlands)* (Vol. 27). Elsevier B.V. https://doi.org/10.1016/j.iot.2024.101318

Nidhom, M., & Murtadho, A. (2025). Does Islam Protect Digital Privacy? An Islamic Studies Approach to Personal Data Protection. *Al-Afham: Journal Of Islamic Studies*, *2*(02). https://doi.org/10.53678/elmadani.v1i02.129

Okdem, S., & Okdem, S. (2024). Artificial Intelligence in Cybersecurity: A Review and a Case Study. *Applied Sciences (Switzerland)*, *14*(22). https://doi.org/10.3390/app142210487

Padela, A. I. (2024). Maqasid al-Shariah and biomedicine: Bridging moral, ethical, and policy discourses. Herndon, VA: International Institute of Islamic Thought.

Putra, T. I. I., Jihadul Islam, A., & Abdul Rahman, A. M. (2024). Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations. *Contemporary Issue on Interfaith Law & Society*, *3*. https://journal.unnes.ac.id/journals/ciils/article/view/31392/5254

Putri, R. R. (2026). *PERLINDUNGAN DATA PRIBADI DAN ETIKA PRIVASI DIGITAL DALAM PERSPEKTIF ISLAM* (Vol. 3, Number 1).

Rafiq, F., Awan, M. J., Yasin, A., Nobanee, H., Zain, A. M., & Bahaj, S. A. (2022). Privacy Prevention of Big Data Applications: A Systematic Literature Review. *SAGE Open*, *12*(2). https://doi.org/10.1177/21582440221096445

Taufiq, M., & Kenyo, A. S. (2025). *The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR* (Vol. 6, Number 2). https://ijble.com/index.php/journal/index

Thoriquttyas, T., & Rohmawati, N. (2026). Maqasid al-Sharia and the digital data ownership: From al-Shatibi to Jasser Auda. *Journal of Islamic Law on Digital Economy and Business*, 168–181. https://doi.org/10.20885/jildeb.vol1.iss2.art5

Tirmidzi, A. (2025). TINJAUAN HUKUM ISLAM TERHADAP PERLINDUNGAN DATA PRIBADI DALAM HUKUM PIDANA ISLAM (STUDI UU NO.27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI). In *Jurnal Wasatiyah: Jurnal Hukum* (Vol. 6, Number 2). www.staimaarifjambi.ac.id

Tsouplaki, A., Fung, C., & Kalloniatis, C. (2025). Enhancing IoT privacy with artificial intelligence: Recent advances and future directions. In *Internet of Things (The Netherlands)* (Vol. 34). Elsevier B.V. https://doi.org/10.1016/j.iot.2025.101752

Undang-Undang Nomor 27 Tahun 2022. (n.d.). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022*.