Current Research on Practice Economics and Sharia Finance (CAPITAL)
Vol. 3, No. 3 Desember 2025
Hal. 06-14

Etika Digitaldan Keamanan Data salam Pemanfaatan Teknologi Informasi di Era Transformasi Digital

Khoirotun Nisa Limbong[1], Stefani[2], Nur Atikah[3], Sofia Damayanti Hasibuan[4], Nurbaiti[5]
[1,2,3,4,5]Universitas Islam Negeri Sumatera Utara
E-mail: khoirotunisa.080905ok@gmail.com[1], stefani@gmail.com[2], nur.atika@gmail.com[3], sopia120224@gmail.com[4], nurbaiti@uinsu.ac.id[5]

Abstrak

Perkembangan teknologi informasi yang semakin pesat telah mendorong terjadinya transformasi digital pada berbagai sektor pelayanan publik, pendidikan, pemerintahan, hingga ruang sosial masyarakat. Perubahan ini tidak hanya menciptakan peluang baru dalam pemanfaatan teknologi, tetapi juga menimbulkan tantangan serius terkait etika digital dan perlindungan data pribadi. Meningkatnya aktivitas digital, penggunaan media sosial, pemanfaatan layanan berbasis cloud, serta digitalisasi layanan kesehatan menunjukkan bahwa kesadaran masyarakat terhadap keamanan informasi masih perlu diperkuat. Sejumlah penelitian menekankan pentingnya pendidikan etika digital, peningkatan literasi keamanan siber, serta penyusunan regulasi yang lebih komprehensif untuk melindungi privasi dan hak-hak pengguna. Selain itu, adopsi teknologi seperti blockchain dan kecerdasan buatan juga membawa implikasi baru terhadap keamanan data. Studi ini mengkaji secara mendalam peran etika digital dan keamanan data dalam mendukung pemanfaatan teknologi informasi yang bertanggung jawab di era transformasi digital. Hasil telaah menunjukkan bahwa penguatan etika digital, penerapan standar perlindungan data, serta peningkatan literasi digital merupakan fondasi penting untuk menciptakan ekosistem digital yang aman, transparan, dan berkelanjutan.

Kata Kunci : Etika digital, keamanan data, perlindungan data pribadi, literasi digital, transformasi digital.

PENDAHULUAN

Transformasi digital tidak hanya mengubah bagaimana masyarakat berinteraksi dengan teknologi, tetapi juga membawa dampak signifikan pada pola pikir, perilaku, serta budaya dalam penggunaan informasi. Seiring meningkatnya intensitas penggunaan platform digital, masyarakat mulai menghadapi persoalan-persoalan moral yang sebelumnya tidak muncul dalam konteks analog. Etika digital kemudian menjadi kerangka penting dalam memastikan bahwa setiap aktivitas teknologi dilakukan secara bertanggung jawab dan tidak menimbulkan kerugian bagi pihak lain. Penelitian terbaru menekankan bahwa pendidikan etika digital harus menjadi bagian integral dalam pembangunan sumber daya manusia di era digital, terutama untuk membentuk kesadaran mengenai batasan-batasan dalam penyebaran informasi, perlindungan privasi, dan perilaku yang dapat diterima secara sosial di ruang digital (Syahda et al., 2024).

Selain itu, peningkatan pengguna internet di Indonesia menunjukkan bahwa isu etika digital tidak lagi menjadi wacana akademik semata, tetapi telah menjadi kebutuhan praktis yang menyentuh berbagai kalangan masyarakat. Penyebaran hoaks, ujaran kebencian, hingga tindakan perundungan digital (cyberbullying) menunjukkan bahwa literasi etika digital masih memerlukan penguatan. Inisiatif untuk meningkatkan kesadaran etika digital telah dilakukan melalui berbagai program edukatif, namun efektivitasnya sangat bergantung pada kemampuan masyarakat dalam menginternalisasi nilai-nilai tersebut (Trisudarmo et al., 2023). Oleh karena itu, peran pendidikan formal, lembaga sosial, serta pemerintah dalam membangun kultur digital yang sehat menjadi faktor yang sangat penting.

Dalam konteks kebebasan berekspresi, etika digital juga memberikan batasan-batasan yang relevan untuk mencegah terjadinya pelanggaran hak orang lain. Media sosial, sebagai ruang ekspresi terbesar dalam era digital, sering kali menjadi arena munculnya konflik-konflik etis. Beberapa penelitian menunjukkan bahwa pengguna media sosial sering kali tidak menyadari bahwa informasi

yang dibagikan dapat menimbulkan konsekuensi hukum maupun sosial, terutama jika informasi tersebut berkaitan dengan data pribadi atau menyerang reputasi seseorang (Mas'ud, 2025). Maka dari itu, pembentukan kesadaran mengenai tanggung jawab digital menjadi fondasi penting bagi terciptanya ruang digital yang aman dan etis.

Isu regulasi juga menjadi bagian fundamental dalam pembahasan mengenai etika digital. Pemerintah telah mulai merespons kebutuhan pengaturan ruang digital melalui penyusunan kebijakan dan regulasi yang berorientasi pada perlindungan data pribadi serta keamanan informasi. Namun, proses implementasinya masih menghadapi berbagai kendala, terutama dalam hal sinkronisasi aturan, pengawasan, serta pemahaman masyarakat terhadap pentingnya kepatuhan hukum dalam aktivitas digital (Dono, 2025). Ketidakseimbangan antara perkembangan teknologi dengan regulasi yang ada menunjukkan adanya urgensi untuk memperkuat kerangka hukum yang mampu mengakomodasi perubahan cepat dalam ekosistem digital.

Dalam ranah perlindungan data pribadi, penelitian menunjukkan bahwa Indonesia masih berada pada tahap awal dalam membangun sistem perlindungan yang terstruktur dan efektif. Sebagian besar masyarakat belum sepenuhnya memahami risiko yang terkait dengan pembagian data pribadi secara terbuka, baik di platform media sosial maupun pada layanan digital lainnya. Kerentanan ini dapat meningkatkan potensi penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu, perlindungan data pribadi tidak hanya membutuhkan kerangka hukum yang kuat tetapi juga kesadaran etis dari setiap individu untuk menjaga informasi pribadinya (Suari & Sarjana, 2023).

Di sisi lain, konsep hukum mengenai data pribadi tidak dapat dilepaskan dari prinsip dasar hak privasi. Hak ini mencakup kendali individu atas bagaimana data mereka dikumpulkan, digunakan, dan disimpan oleh lembaga atau platform digital. Penelitian hukum menjelaskan bahwa perlindungan data pribadi merupakan bagian integral dari perlindungan hak asasi manusia, sehingga negara memiliki tanggung jawab untuk memastikan bahwa setiap warga negara mendapatkan perlindungan terhadap penyalahgunaan data (Kusnadi, 2021). Dalam banyak kasus, minimnya literasi hukum masyarakat menyebabkan mereka tidak memahami hak-hak yang dimiliki terkait pengelolaan data pribadi.

Dari perspektif regulasi, Indonesia menghadapi tantangan dalam menyeimbangkan antara perlindungan data pribadi dan kebutuhan industri digital. Ketika sektor teknologi berkembang pesat, sering kali terjadi ketidakseimbangan antara kepentingan bisnis yang mengumpulkan data dalam jumlah besar dan kebutuhan masyarakat terhadap privasi. Perbandingan dengan negara lain seperti Uni Eropa memperlihatkan bahwa perlindungan data pribadi seharusnya mengutamakan transparansi, persetujuan pengguna, dan pembatasan penggunaan data sesuai tujuan awal pengumpulan (Ramadhani, 2021). Kondisi ini mendorong kebutuhan harmonisasi antara perkembangan industri digital dan kepentingan publik yang lebih luas.

Dalam konteks keamanan data, perkembangan teknologi membawa tantangan baru yang semakin kompleks. Implementasi teknologi blockchain telah menjadi solusi potensial dalam memperkuat keamanan data karena sifatnya yang terdesentralisasi dan tidak mudah dimanipulasi. Namun, adopsi teknologi ini masih berada pada tahap awal dan membutuhkan pemahaman yang komprehensif dari aspek teknis maupun etis (Suryawijaya, 2023). Di sisi lain, penggunaan teknologi cloud computing juga mendorong kebutuhan untuk menerapkan kebijakan keamanan yang ketat mengingat data semakin banyak disimpan dan diproses secara daring. Organisasi yang tidak memiliki standar keamanan tinggi akan lebih rentan terhadap ancaman siber seperti peretasan dan kebocoran data (Pandu et al., 2024).

Dalam sektor pendidikan tinggi dan organisasi kampus, penggunaan sistem digital telah berkembang pesat terutama setelah meningkatnya kebutuhan pembelajaran daring. Hal ini menuntut institusi pendidikan untuk memperkuat mekanisme keamanan sistem informasi mereka, terutama dengan pemanfaatan kecerdasan buatan sebagai alat pendukung operasional. Namun, teknologi AI juga menghadirkan potensi risiko baru seperti bias algoritmik, penyalahgunaan data pengguna, serta pelanggaran privasi jika tidak diatur dengan baik. Oleh sebab itu, transformasi digital dalam lingkungan kampus perlu disertai dengan penerapan prinsip-prinsip etika digital yang jelas (Santoso, 2025).

Selain itu, literasi digital menjadi fondasi penting dalam mendukung keamanan dan etika penggunaan teknologi. Remaja sebagai pengguna aktif media sosial berada dalam kelompok paling rentan terhadap ancaman siber seperti pencurian data, intimidasi digital, dan penyebaran informasi palsu. Penelitian menunjukkan bahwa program literasi digital yang komprehensif dapat meningkatkan

kemampuan remaja dalam mengidentifikasi risiko keamanan serta memperkuat perilaku etis dalam penggunaan media sosial (Effendy, 2024). Penguatan literasi digital bukan hanya fokus pada kemampuan teknis, tetapi juga pemahaman mendalam mengenai etika, privasi, dan keamanan informasi.

Transformasi digital pada layanan publik juga menunjukkan bahwa keamanan data tidak boleh dipandang sebagai aspek teknis semata, tetapi sebagai bagian dari tata kelola pemerintahan yang baik. Ketidakmampuan pemerintah daerah dalam melindungi data warganya dapat menurunkan kepercayaan publik dan menghambat efektivitas layanan digital. Oleh karena itu, strategi keamanan data harus dijadikan prioritas utama dalam percepatan transformasi digital pemerintah (Salijah et al., 2025).

Digitalisasi layanan kesehatan turut membuka diskusi etika yang kompleks, terutama mengenai pelindungan data pasien yang bersifat sangat sensitif. Sistem kesehatan digital perlu dirancang dengan menerapkan prinsip keamanan berlapis, enkripsi data, serta pembatasan akses agar data pasien tidak disalahgunakan. Di beberapa kasus, lemahnya pemahaman petugas kesehatan tentang literasi digital menyebabkan data pasien menjadi rentan, sehingga institusi kesehatan perlu meningkatkan standar pengelolaan data dan pelatihan keamanan digital (Khoirunisah, 2025).

Pada titik ini, tampak jelas bahwa pembahasan mengenai etika digital dan keamanan data tidak dapat dilakukan secara parsial. Etika digital tidak hanya berbicara mengenai bagaimana seseorang berperilaku di ruang digital, tetapi juga menyangkut tanggung jawab organisasi, pemerintah, penyedia layanan, dan lembaga pendidikan dalam membangun sistem yang aman dan etis. Dengan meningkatnya kompleksitas ancaman digital, kebutuhan untuk memperkuat mekanisme perlindungan data serta menerapkan standar etika dalam penggunaan teknologi menjadi semakin mendesak. Oleh karena itu, bagian pendahuluan ini menjadi landasan penting untuk memahami bagaimana etika digital dan keamanan data saling berkaitan dalam membentuk ekosistem digital yang sehat, aman, dan berkelanjutan.

TINJAUAN TEORETIS

Etika Digital

Etika digital merupakan seperangkat prinsip moral yang mengatur perilaku individu dan kelompok ketika berinteraksi dengan teknologi dan ruang digital. Dalam era transformasi digital yang semakin luas, etika digital berfungsi sebagai landasan untuk mengarahkan pengguna agar bertindak secara bertanggung jawab, aman, dan menghormati hak-hak orang lain. Penelitian menegaskan bahwa etika digital tidak hanya berkaitan dengan perilaku dalam bermedia sosial, tetapi juga mencakup bagaimana individu memperlakukan data, menghargai privasi, serta memahami batasan dalam penggunaan teknologi (Syahda et al., 2024).

Perilaku tidak etis di ruang digital kini muncul dalam berbagai bentuk seperti penyebaran informasi palsu, perundungan digital, ujaran kebencian, hingga penyalahgunaan data pribadi. Oleh karena itu, pendidikan etika digital menjadi kebutuhan mendasar dalam masyarakat modern. Penanaman nilai etis sejak dini akan membantu individu memahami konsekuensi sosial dan hukum dari aktivitas mereka di dunia maya. Trisudarmo dan koleganya menggarisbawahi perlunya peningkatan kesadaran masyarakat melalui pendekatan edukatif yang sistematis agar nilai-nilai etika digital dapat diterapkan secara konsisten (Trisudarmo et al., 2023).

Selain itu, dilema etis juga muncul dalam konteks kebebasan berekspresi. Media sosial memberikan ruang luas bagi individu untuk berpendapat, namun kebebasan tersebut sering kali tidak disertai tanggung jawab. Pengguna kerap melupakan bahwa konten digital dapat berdampak pada orang lain, bahkan berpotensi menciptakan pelanggaran privasi atau reputasi. Mas'ud menegaskan bahwa etika digital perlu menyeimbangkan antara kebebasan ekspresi dan kewajiban menjaga hak-hak pengguna lain (Mas'ud, 2025).

Etika digital tidak hanya berlaku pada tingkat individu, tetapi juga pada organisasi, institusi pendidikan, pemerintah, dan penyedia layanan digital. Dalam lingkup kelembagaan, etika digital menuntut adanya transparansi, perlindungan data, dan tanggung jawab dalam memproses informasi pengguna. Dono menjelaskan bahwa regulasi dan tata kelola komunikasi digital perlu dikembangkan secara komprehensif agar prinsip etika dapat diintegrasikan ke seluruh lapisan sistem (Dono, 2025).

Keamanan Data

Keamanan data (data security) adalah upaya untuk melindungi informasi dari akses ilegal, penyalahgunaan, atau kerusakan. Dalam ekosistem digital modern, keamanan data menjadi aspek kritis karena meningkatnya volume data yang dikumpulkan, disimpan, dan diproses melalui sistem informasi dan aplikasi berbasis internet. Berbagai penelitian menekankan pentingnya membangun sistem yang mampu menyediakan proteksi berlapis terhadap serangan siber, baik melalui enkripsi, autentikasi, pengawasan jaringan, maupun kebijakan internal (Suari & Sarjana, 2023)

Kerentanan digital semakin besar akibat banyaknya platform yang mengumpulkan data pribadi tanpa kontrol keamanan yang memadai. Kebocoran data menjadi salah satu ancaman serius yang dapat menyebabkan kerugian signifikan, mulai dari pencurian identitas, penipuan, hingga manipulasi integritas sistem digital. Kusnadi menyoroti bahwa perlindungan data pribadi sangat berkaitan dengan hak privasi, sehingga keamanan data harus dipandang sebagai bagian dari upaya melindungi hak asasi manusia (Kusnadi, 2021).

Di sisi regulasi, Indonesia telah mengembangkan kerangka hukum yang lebih kuat terkait perlindungan data pribadi, namun implementasinya masih berada dalam tahap transisi. Tantangan muncul dalam bentuk rendahnya literasi hukum masyarakat, lemahnya penegakan regulasi, serta kompleksitas teknologi yang terus berkembang. Sinaga menjelaskan bahwa formulasi legislasi yang ada masih memerlukan penguatan agar sesuai dengan prinsip-prinsip perlindungan data internasional (Sinaga, 2020).

Dalam konteks perbandingan global, Ramadhani menelaah bagaimana GDPR di Uni Eropa memberikan contoh model perlindungan data yang lebih komprehensif, terutama dalam hal transparansi pengolahan data, batasan penggunaan, dan persetujuan pengguna (Ramadhani, 2021). Temuan ini menunjukkan bahwa Indonesia perlu menyesuaikan strategi perlindungan data dengan standar global untuk meningkatkan kepercayaan masyarakat terhadap layanan digital.

Selain faktor regulasi, perkembangan teknologi seperti blockchain, cloud computing, dan kecerdasan buatan (AI) telah membawa dinamika baru terhadap keamanan data. Suryawijaya menemukan bahwa blockchain dapat meningkatkan keamanan melalui sistem penyimpanan terdesentralisasi yang sulit diretas (Suryawijaya, 2023). Namun, implementasi blockchain memerlukan kesiapan teknis serta pemahaman etis mengenai konsekuensi penggunaan teknologi tersebut.

Dalam penggunaan cloud computing, masalah keamanan data sering kali muncul akibat kurangnya pemahaman organisasi terhadap risiko penyimpanan data secara daring. Pandu dan koleganya menjelaskan bahwa cloud dapat meningkatkan efisiensi dan aksesibilitas data, tetapi memerlukan kebijakan keamanan yang ketat untuk mencegah kebocoran dan serangan siber (Pandu et al., 2024).

Literasi Digital dan Kesadaran Keamanan Siber

Literasi digital merupakan kemampuan individu dalam menggunakan teknologi informasi secara efektif, kritis, dan aman. Literasi digital tidak hanya mencakup keterampilan teknis, tetapi juga kesadaran akan risiko yang ada di ruang digital. Effendy menemukan bahwa remaja merupakan kelompok dengan risiko tertinggi terhadap ancaman siber, sehingga pendidikan literasi digital perlu diarahkan pada pemahaman tentang keamanan informasi, privasi, serta perilaku etis dalam menggunakan media sosial (Effendy, 2024).

Komponen literasi digital yang menyentuh aspek keamanan meliputi pemahaman tentang serangan siber, cara melindungi akun, manajemen kata sandi, hingga mengenali indikasi phishing. Anjani dan Prasetya juga menyoroti pentingnya edukasi literasi digital bagi masyarakat umum agar mereka memahami konsekuensi berbagi data sembarangan atau mengakses platform yang tidak aman (Anjani & Prasetya, 2024).

Kesadaran keamanan siber juga berpengaruh besar terhadap kemampuan masyarakat dalam mengurangi risiko digital. Banyak individu tidak menyadari bahwa aktivitas sehari-hari seperti mengklik tautan tidak aman, mengunduh aplikasi ilegal, atau membagikan informasi sensitif dapat membuka peluang serangan. Oleh karena itu, pembentukan perilaku digital yang aman menjadi bagian inti dalam literasi digital.

Etika dan Keamanan Digital dalam Sektor Pemerintahan

Dalam sektor pemerintahan, digitalisasi layanan publik menuntut adanya kebijakan dan infrastruktur keamanan yang lebih kuat. Pemerintah daerah maupun pusat harus memastikan bahwa data masyarakat terlindungi dari ancaman peretasan dan penyalahgunaan. Salijah dan koleganya menjelaskan bahwa keamanan data merupakan pilar strategis dalam mempercepat transformasi digital pemerintahan, terutama untuk menjaga kepercayaan publik (Salijah et al., 2025).

Layanan publik berbasis digital sering kali rentan karena minimnya pengawasan, kurangnya standardisasi keamanan, serta lemahnya kompetensi digital aparatur. Oleh karena itu, pemerintah perlu mengembangkan pedoman tata kelola keamanan informasi yang komprehensif, meliputi manajemen risiko, audit keamanan, penanganan insiden, serta edukasi bagi pegawai.

Etika dan Keamanan Digital dalam Layanan Kesehatan

Digitalisasi layanan kesehatan (e-health) membuka banyak peluang, namun juga menghadirkan tantangan terkait etika dan perlindungan data pasien. Data medis dianggap sebagai informasi paling sensitif, sehingga kebocoran dapat menyebabkan dampak sosial dan psikologis yang besar. Khoirunisah mengungkapkan bahwa institusi kesehatan masih menghadapi hambatan dalam menerapkan standar keamanan data yang memadai, baik dari sisi infrastruktur maupun literasi SDM (Khoirunisah, 2025).

Konsep informed consent dalam layanan digital juga menjadi isu penting, di mana pasien harus memahami bagaimana data mereka disimpan dan diproses. Tanpa transparansi dan perlindungan memadai, digitalisasi kesehatan dapat menimbulkan risiko etik yang signifikan.

Teknologi AI dan Tantangan Etis

Penggunaan kecerdasan buatan dalam sistem informasi membawa peluang untuk meningkatkan efisiensi, namun juga menghadirkan risiko etik seperti bias algoritmik, penyalahgunaan data, dan ketidaktransparanan proses pengambilan keputusan. Santoso menekankan perlunya regulasi dan etika yang jelas dalam pemanfaatan AI, terutama pada lingkungan pendidikan dan institusi publik (Santoso, 2025). Penggunaan AI harus selalu memperhatikan prinsip *fairness*, *accountability*, *dan transparency*, terutama ketika melibatkan pengolahan data pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode studi pustaka (library research) yang berfokus pada penelaahan berbagai sumber ilmiah untuk memahami secara menyeluruh bagaimana etika digital dan keamanan data menjadi isu penting dalam pemanfaatan teknologi informasi di era transformasi digital. Pemilihan metode ini didasarkan pada pertimbangan bahwa topik yang dikaji bersifat konseptual, multidisipliner, dan terus berkembang, sehingga membutuhkan analisis teori yang berasal dari beragam penelitian sebelumnya. Data penelitian dikumpulkan melalui penelusuran artikel jurnal yang relevan menggunakan Google Scholar dengan kata kunci seperti “etika digital”, “keamanan data”, “perlindungan data pribadi”, dan “literasi digital”.

Analisis dilakukan melalui teknik content analysis, yaitu metode yang memfokuskan pada pemahaman isi literatur dan mengidentifikasi hubungan konseptual antara etika digital, perilaku pengguna, bentuk ancaman siber, kebijakan perlindungan data, dan kesiapan institusi digital. Teknik ini melibatkan beberapa langkah, mulai dari identifikasi konsep utama seperti privasi, tanggung jawab digital, perlindungan data, hingga keamanan informasi; pengelompokan temuan berdasarkan perspektif sosial, teknologi, hukum, dan kelembagaan; serta sintesis teoritis untuk menyusun pemahaman yang lebih komprehensif tentang bagaimana konsep-konsep tersebut saling terkait.

Pendekatan ini memungkinkan peneliti mengkaji isu secara mendalam tanpa terhambat oleh keterbatasan data lapangan, karena seluruh fenomena telah banyak dibahas dalam penelitian sebelumnya. Studi pustaka juga dipilih karena dinilai paling tepat untuk topik yang berkaitan dengan perubahan perilaku digital, inovasi teknologi, serta perkembangan kebijakan digital yang terus berubah secara cepat. Dengan mengintegrasikan berbagai temuan penelitian, metode ini menghasilkan gambaran yang lebih luas tentang bagaimana etika digital dan keamanan data harus dikelola dalam konteks sosial dan teknologi modern, termasuk perlunya peningkatan literasi digital, penegakan regulasi privasi, dan penguatan kebijakan keamanan informasi pada berbagai sektor. Secara keseluruhan, metode penelitian ini memberikan landasan teoretis yang solid dan sistematis yang dapat dipertanggungjawabkan secara

akademik, sehingga mampu mendukung analisis mendalam pada pembahasan selanjutnya mengenai hubungan antara etika digital, keamanan data, dan dinamika transformasi digital.

HASIL DAN PEMBAHASAN

Etika Digital sebagai Landasan Perilaku Pengguna dalam Ekosistem Digital

Percepatan transformasi digital dalam berbagai sektor kehidupan telah mengubah pola perilaku masyarakat secara signifikan. Aktivitas harian seperti komunikasi, transaksi ekonomi, pembelajaran, dan pelayanan publik kini dilakukan melalui media digital yang terhubung satu sama lain. Perubahan besar ini menuntut pengguna untuk memahami etika digital sebagai pedoman dalam berperilaku di ruang maya. Etika digital tidak hanya sekadar sopan santun dalam bermedia sosial, tetapi mencakup kesadaran akan tanggung jawab moral ketika mengakses, mengelola, dan membagikan informasi digital. Syahda dan rekan-rekannya menegaskan bahwa etika digital merupakan salah satu kompetensi yang harus diajarkan kepada generasi sekarang, terutama karena perilaku online seseorang memiliki dampak langsung terhadap dirinya maupun orang lain (Syahda et al., 2024). Hal ini menunjukkan bahwa etika digital tidak lagi menjadi wacana normatif, tetapi telah menjadi kebutuhan praktis dalam kehidupan sehari-hari.

Rendahnya pemahaman masyarakat mengenai etika digital terlihat dari maraknya perilaku tidak etis seperti penyebaran hoaks, ujaran kebencian, perundungan digital, dan pelanggaran privasi. Menurut Trisudarmo, sebagian besar pengguna internet tidak memiliki kesadaran yang memadai tentang dampak sosial dan psikologis dari perilaku digital mereka, sehingga tindakan yang dilakukan di dunia maya kerap tidak mempertimbangkan konsekuensi yang mungkin timbul (Trisudarmo et al., 2023). Ini menunjukkan bahwa tingkat literasi digital masyarakat masih belum sejalan dengan pertumbuhan akses internet yang semakin luas. Mas'ud juga menegaskan bahwa media sosial sering kali menjadi ruang tempat dilema etika muncul karena pengguna merasa lebih bebas mengekspresikan diri tanpa kontrol sosial yang ketat, sehingga batas antara kebebasan berekspresi dan tindakan yang merugikan orang lain menjadi kabur (Mas'ud, 2025).

Selain perilaku individu, etika digital juga menuntut institusi, organisasi, dan penyedia layanan digital untuk bertanggung jawab dalam mengelola data, menyediakan layanan yang aman, serta menjaga transparansi. Dono menyatakan bahwa pengelolaan komunikasi digital membutuhkan regulasi dan tata kelola yang baik untuk memastikan bahwa penyedia layanan tidak menyalahgunakan informasi pengguna (Dono, 2025). Dengan demikian, etika digital tidak hanya bersifat personal, tetapi juga institusional. Institusi pendidikan, organisasi publik, dan perusahaan teknologi memiliki kewajiban moral untuk menerapkan standar etika dalam operasional digital mereka.

Kesadaran terhadap etika digital menjadi semakin penting seiring meningkatnya ketergantungan masyarakat pada teknologi. Banyak interaksi digital kini berlangsung tanpa pengawasan langsung, sehingga perilaku yang tidak etis dapat menyebar lebih cepat dan berdampak lebih luas. Oleh karena itu, membangun budaya etika digital memerlukan kolaborasi antara pemerintah, lembaga pendidikan, industri teknologi, dan masyarakat. Prinsip-prinsip etika seperti kejujuran, tanggung jawab, kehati-hatian, dan penghormatan terhadap privasi harus terus ditekankan agar setiap individu dapat menjadi pengguna digital yang bijak.

Ancaman Keamanan Data dan Perlindungan Informasi Pribadi dalam Transformasi Digital

Seiring dengan meningkatnya intensitas penggunaan layanan digital, keamanan data menjadi salah satu isu paling mendesak dalam ekosistem digital. Data pengguna, baik berupa informasi pribadi, riwayat transaksi, atau data kesehatan, menjadi aset berharga yang kerap menjadi sasaran kejahatan digital. Suari dan Sarjana menunjukkan bahwa kebocoran data semakin sering terjadi karena masih banyak platform yang belum menerapkan sistem keamanan yang memadai (Suari & Sarjana, 2023). Hal ini mengakibatkan pengguna rentan terhadap penyalahgunaan data seperti pencurian identitas, pemalsuan data, hingga penipuan online.

Keamanan data memiliki hubungan langsung dengan hak privasi pengguna. Dalam perspektif hukum, perlindungan data pribadi merupakan bagian dari perlindungan hak asasi manusia. Kusnadi menekankan bahwa data pribadi harus diperlakukan sebagai aset sensitif yang harus dilindungi oleh negara melalui regulasi perlindungan data yang kuat (Kusnadi, 2021). Sayangnya, regulasi yang ada saat ini belum sepenuhnya mampu mengakomodasi dinamika perubahan teknologi. Sinaga menjelaskan

bahwa sistem legislasi perlindungan data di Indonesia masih berada dalam tahap pengembangan dan memerlukan revisi agar dapat mengantisipasi ancaman digital modern (Sinaga, 2020).

Banyaknya kasus kebocoran data menunjukkan bahwa perlindungan data tidak cukup hanya dari sisi hukum, tetapi juga memerlukan penguatan teknologi. Teknologi blockchain, misalnya, menawarkan sistem keamanan yang lebih sulit diretas karena struktur datanya yang terdesentralisasi dan kedap manipulasi. Suryawijaya menyatakan bahwa blockchain memiliki potensi besar untuk digunakan dalam sektor-sektor yang mengelola informasi sensitif, terutama dalam mengurangi risiko penyalahgunaan data (Suryawijaya, 2023).

Selain blockchain, penggunaan cloud computing juga telah menjadi bagian penting dari digitalisasi. Namun, penggunaan cloud yang tidak disertai standar keamanan yang tepat dapat meningkatkan risiko kebocoran data. Pandu dan rekannya menemukan bahwa banyak organisasi belum menerapkan manajemen risiko yang cukup matang dalam penggunaan layanan cloud, sehingga data yang disimpan di server daring menjadi rentan (Pandu et al., 2024).

Tidak hanya sektor pendidikan dan bisnis, pemerintahan pun menghadapi tantangan besar dalam menjaga keamanan data masyarakat. Salijah menyoroti bahwa sistem keamanan layanan publik digital masih sangat bervariasi dan sering kali belum memenuhi standar minimum keamanan informasi (Salijah et al., 2025). Hal ini menunjukkan bahwa keamanan data bukan hanya persoalan teknologi, tetapi juga tata kelola dan kapasitas sumber daya manusia.

Sektor kesehatan menjadi salah satu sektor yang menghadapi risiko tertinggi terkait keamanan data. Data kesehatan sangat sensitif dan dapat menimbulkan dampak serius jika bocor. Khoirunisah menemukan bahwa institusi kesehatan memiliki tantangan besar dalam menjaga keamanan data pasien karena rendahnya literasi digital tenaga kesehatan serta lemahnya infrastruktur keamanan (Khoirunisah, 2025).

Literasi Digital dan Perilaku Pengguna sebagai Penentu Keamanan Ekosistem Digital

Literasi digital merupakan salah satu pilar paling fundamental dalam menjaga keamanan data dan etika berinternet, terutama di tengah derasnya arus transformasi digital. Walaupun teknologi keamanan data seperti enkripsi, firewall, atau blockchain terus berkembang, faktor manusia tetap menjadi gerbang utama yang menentukan keberhasilan sistem keamanan digital. Tanpa literasi digital yang memadai, berbagai bentuk ancaman siber seperti phishing, peretasan akun, pencurian identitas, manipulasi data, hingga penyebaran malware dapat terjadi dengan sangat mudah. Menurut Effendy, rendahnya literasi digital pengguna – terutama kalangan remaja dan generasi muda – menjadi penyebab utama meningkatnya kasus kejahatan digital yang menyasar kelompok rentan ini (Effendy, 2024). Hal ini menunjukkan bahwa literasi digital harus dipahami bukan semata-mata kemampuan menggunakan perangkat, tetapi juga kesadaran terhadap ancaman, sikap kritis dalam menerima informasi, dan kemampuan melindungi jejak digital.

Perilaku pengguna yang tidak aman masih menjadi masalah besar dalam ekosistem digital. Banyak individu tidak sadar bahwa tindakan sederhana seperti membagikan foto identitas, lokasi pribadi, atau informasi sensitif di media sosial dapat menimbulkan risiko serius. Anjani dan Prasetya menjelaskan bahwa sebagian besar pengguna tidak memiliki pemahaman mendalam tentang privasi digital, sehingga mereka cenderung membagikan data tanpa mempertimbangkan siapa saja yang dapat melihat, menyimpan, atau menyalahgunakan data tersebut (Anjani & Prasetya, 2024). Rendahnya kesadaran ini diperparah oleh budaya digital yang semakin konsumtif, di mana pengguna lebih mementingkan kenyamanan dan kecepatan akses dibandingkan keamanan.

Di sisi lain, literasi digital memiliki hubungan erat dengan kemampuan mengidentifikasi ancaman siber. Banyak kasus pencurian data terjadi bukan karena lemahnya sistem, tetapi karena pengguna mudah terperangkap dalam taktik social engineering, seperti link palsu, phishing berbentuk email resmi, atau aplikasi tidak terpercaya. Pengguna yang memiliki literasi keamanan digital yang baik akan lebih waspada terhadap modus penipuan digital dan mampu mengambil langkah preventif seperti memverifikasi sumber, menghindari tautan mencurigakan, serta menggunakan autentikasi dua faktor untuk menjaga keamanan akun. Dalam konteks ini, literasi digital bukan hanya pengetahuan teknis, tetapi juga mencakup kemampuan berpikir kritis dan reflektif dalam menghadapi informasi yang diterima.

Pentingnya literasi digital juga terlihat dalam perilaku penggunaan media sosial. Platform media sosial sangat mudah menjadi sarana penyebaran misinformasi dan konten merugikan. Tanpa literasi digital, pengguna cenderung menyebarkan informasi tanpa verifikasi, yang kemudian memperburuk kualitas ruang digital. Hal ini berkaitan erat dengan etika digital yang dibahas pada bagian sebelumnya. Syahda dan koleganya menjelaskan bahwa etika digital dan literasi digital harus berjalan bersamaan agar pengguna dapat memahami bukan hanya teknis penggunaan media, tetapi juga nilai-nilai moral yang diperlukan untuk menjaga hubungan sosial di ranah digital (Syahda et al., 2024). Artinya, literasi digital tidak dapat dipisahkan dari kesadaran etika dalam mengelola informasi dan teknologi.

Selain itu, aspek psikologis juga memengaruhi perilaku pengguna. Remaja, misalnya, menggunakan media sosial sebagai ruang eksplorasi diri, sehingga mereka sering kali tidak mempertimbangkan risiko ketika mengunggah foto, data pribadi, atau berinteraksi dengan orang asing. Menurut Effendy, kelompok ini sangat rentan terhadap pengaruh sosial di internet, sehingga mereka lebih mudah terpapar penipuan digital, cyberbullying, atau eksploitasi data pribadi (Effendy, 2024). Oleh karena itu, pendidikan literasi digital perlu diarahkan tidak hanya pada aspek teknis, tetapi juga pada pembentukan karakter digital dan kemampuan menghadapi tekanan sosial online.

Dalam konteks nasional, rendahnya literasi digital juga dipengaruhi oleh ketimpangan akses pendidikan dan teknologi. Di wilayah perkotaan, pengguna mungkin memiliki akses lebih baik terhadap teknologi dan informasi, tetapi di wilayah pedesaan, literasi digital masih tertinggal. Hal ini menciptakan kesenjangan dalam kemampuan melindungi data dan memahami risiko digital. Dampaknya, masyarakat yang minim literasi digital cenderung menjadi target empuk bagi para pelaku kejahatan siber yang memanfaatkan ketidaktahuan pengguna. Oleh sebab itu, pemerintah perlu memastikan pemerataan pendidikan digital sebagai upaya perlindungan siber nasional.

Program literasi digital juga harus mempertimbangkan berbagai kelompok masyarakat, tidak hanya pelajar dan remaja. Misalnya, pekerja kantor perlu memahami keamanan siber untuk melindungi data perusahaan; orang tua perlu memahami risiko digital bagi anak-anak; pedagang online harus mengetahui cara aman bertransaksi; sementara pelaku UMKM harus mengetahui cara mengelola data pelanggan agar tidak disalahgunakan. Anjani dan Prasetya menekankan bahwa literasi digital masyarakat umum harus ditingkatkan agar mereka memahami konsep privasi digital dan keamanan data dalam kehidupan sehari-hari (Anjani & Prasetya, 2024). Ini menunjukkan bahwa literasi digital adalah konsep universal yang berlaku pada semua sektor dan usia.

Selain pengguna individu, organisasi juga memainkan peran besar dalam membentuk budaya literasi digital. Banyak organisasi belum memberikan pelatihan keamanan digital yang memadai kepada karyawan, sehingga terjadi kelalaian internal yang menyebabkan kebocoran data. Misalnya, penggunaan kata sandi lemah, akses perangkat tanpa pengamanan, atau membuka email mencurigakan dari alamat tak dikenal. Ketidaksadaran ini dapat menyebabkan kerugian besar bagi organisasi. Oleh karena itu, pelatihan reguler mengenai keamanan digital harus menjadi kebijakan setiap institusi.

Pada akhirnya, literasi digital tidak hanya berfungsi sebagai alat proteksi individual, tetapi juga sebagai mekanisme pertahanan kolektif dalam ekosistem digital nasional. Semakin tinggi literasi digital masyarakat, semakin kecil peluang bagi pelaku kejahatan siber untuk mengeksploitasi kelemahan pengguna. Dengan kata lain, literasi digital yang kuat akan menciptakan ekosistem digital yang lebih aman, sehat, dan berkualitas.

KESIMPULAN DAN SARAN

Transformasi digital telah memberikan kemajuan yang signifikan bagi berbagai sektor kehidupan, mulai dari pendidikan, pemerintahan, kesehatan, bisnis, hingga interaksi sosial. Namun, perkembangan tersebut juga membawa tantangan yang tidak bisa diabaikan, khususnya dalam aspek etika digital dan keamanan data. Berdasarkan pembahasan yang telah dilakukan, dapat disimpulkan bahwa etika digital merupakan fondasi utama dalam penggunaan teknologi informasi secara bertanggung jawab. Etika digital tidak hanya mencakup tata krama berkomunikasi di ruang maya, tetapi juga mencakup kemampuan menjaga privasi, menghormati hak orang lain, serta memahami dampak sosial dari setiap tindakan digital. Masyarakat perlu menyadari bahwa perilaku online memiliki konsekuensi yang sama pentingnya dengan tindakan di dunia nyata.

Selain itu, keamanan data menjadi komponen krusial yang menentukan keberhasilan transformasi digital. Data pribadi kini menjadi aset berharga yang rawan disalahgunakan apabila tidak dilindungi secara memadai. Tantangan keamanan data muncul dalam bentuk ancaman siber, kebocoran data, penyalahgunaan informasi, dan lemahnya regulasi maupun infrastruktur keamanan digital. Perlindungan data tidak hanya memerlukan teknologi yang canggih, tetapi juga regulasi yang tegas serta kesadaran individu untuk menjaga keamanan identitas digital masing-masing. Di sisi lain, literasi digital terbukti menjadi penentu utama dalam membangun ekosistem digital yang aman dan sehat.

Masyarakat yang memiliki literasi digital yang baik akan lebih mampu melindungi diri dari ancaman siber, lebih bijak dalam membagikan informasi, serta lebih kritis dalam menerima dan memproses data di dunia maya. Literasi digital yang kuat menjadi benteng pertahanan pertama dalam mengurangi risiko-risiko digital yang terus berkembang.Secara keseluruhan, keberhasilan transformasi digital tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh perilaku penggunanya, kebijakan yang diterapkan, serta kualitas literasi digital masyarakat. Etika digital, keamanan data, dan literasi digital harus berjalan selaras agar mampu menciptakan ekosistem digital yang aman, berkelanjutan, dan mampu memberikan manfaat optimal bagi seluruh lapisan masyarakat.

DAFTAR PUSTAKA

Anjani, N., & Prasetya, A. (2024). Pemanfaatan teknologi informasi dalam edukasi literasi digital untuk peningkatan keamanan data masyarakat. *Merkurius: Jurnal Ilmu Komunikasi dan Teknologi Informasi*, *6*(2), 45–57.

Dono, L. (2025). Etika dan regulasi komunikasi digital. *Madhangi: Jurnal Ilmu Komunikasi*.

Effendy, M. Y. (2024). Literasi digital keamanan siber pada remaja pengguna media sosial. *Wacana Publik: Jurnal Ilmu Politik dan Komunikasi*, *2*(1), 1–12.

Khoirunisah, N. (2025). Digitalisasi layanan kesehatan: Tantangan etika dan keamanan data pasien. *Presidensial*, *2*(2), 263–273.

Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al-Wasath: Jurnal Hukum Islam*, *2*(1), 45–62.

Mas'ud, F. (2025). Etika dalam media sosial antara kebebasan ekspresi dan tanggung jawab digital. *Jurnal Ilmu Manajemen dan Multimedia (JIMMI)*.

Pandu, R. M., Widodo, D. S. A., & Muttaqin, H. A. (2024). Manajemen keamanan data dalam era transformasi digital dan cloud computing. *Jurnal JIFORTY*, *5*(2), 145–154.

Ramadhani, S. A. (2021). Komparasi pengaturan perlindungan data pribadi di Indonesia dan Uni Eropa. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *3*(1), 1–20.

Salijah, E., Basid, A., & Annas, A. (2025). Keamanan data sebagai pilar strategis percepatan transformasi digital Pemerintah Kota Makassar. *JIAP: Jurnal Ilmu Administrasi Publik*.

Santoso, I. (2025). Model transformasi keamanan digital dalam jaringan kampus berbasis AI. *Jurnal Rekayasa Komputer (JAREKOM)*.

Sinaga, E. M. C. (2020). Formulasi legislasi perlindungan data pribadi di Indonesia. *Jurnal Rechtsvinding*, *9*(1), 63–82.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–144.

Suryawijaya, T. W. E. (2023). Memperkuat keamanan data melalui teknologi blockchain: Mengeksplorasi implementasi sukses dalam transformasi digital di Indonesia. *JSKP: Jurnal Studi Kebijakan Publik*, *2*(1), 55–67.

Syahda, F. L., Nur'aisyah, Y., & Rachman, I. F. (2024). Pentingnya pendidikan etika digital dalam konteks SDGs 2030. *Perspektif: Jurnal Pendidikan dan Ilmu Bahasa*, *2*(2), 1–16.

Trisudarmo, R., Wati, D. P., & Irawan, D. (2023). Peningkatan kesadaran dan penerapan etika digital di kalangan pengguna internet. *Jurnal Pasopati*, *5*(3).