Scripta Economica:
Journal of Economics, Management, and Accounting
Vol 1 No 2 November 2025, Hal 71-79
ISSN: 3110-0848 (Print) ISSN: 3109-970X (Electronic)
Open Access: https://scriptaintelektual.com/scripta-economica

Perlindungan Data Pribadi sebagai Pilar Keberlanjutan dan Pertumbuhan Ekonomi Digital di Indonesia

Unggul Sagena[1*], Tukina[2], Tia Ramda Sari[3]
[1] Southeast Asia Freedom of Expression Network (SAFEnet), Indonesia
[2] Binus University, Indonesia
[3] Universitas Jambi, Indonesia
email: unggul@safenet.or.id[1]

Article Info :
Received:
24-9-2025
Revised:
25-9-2025
Accepted:
26-10-2025

Abstract

Indonesia's rapid digital economic development has positioned personal data as a strategic asset in supporting innovation, efficiency, and public trust in digital services. This study aims to analyze the effectiveness of personal data protection implementation in supporting the stability and growth of Indonesia's digital economy. The method used is a descriptive qualitative approach through secondary data analysis from official government reports, academic publications, and international research institutions. The results show that although regulations have created a comprehensive legal framework, their effectiveness is still hampered by delays in establishing an independent supervisory agency, limited human and technical resources, and low public and business awareness of personal data protection. The economic impact of weak implementation is reflected in declining public trust, increased investment risk, and reduced national digital competitiveness. The success of personal data protection must be seen as a key prerequisite for the sustainability of Indonesia's digital economy through collaboration between the government, the private sector, and the public in creating a secure, transparent, and competitive digital ecosystem.

Keywords: *Personal Data Protection, Digital Economy, Cybersecurity, Digital Investment, Public Trust.*

Akbstrak

Perkembangan ekonomi digital Indonesia yang pesat menempatkan data pribadi sebagai aset strategis dalam menopang inovasi, efisiensi, dan kepercayaan publik terhadap layanan digital. Penelitian ini bertujuan untuk menganalisis efektivitas implementasi perlindungan data pribadi dalam mendukung stabilitas dan pertumbuhan ekonomi digital Indonesia. Metode yang digunakan adalah pendekatan kualitatif deskriptif melalui analisis data sekunder dari laporan resmi pemerintah, publikasi akademik, dan lembaga riset internasional. Hasil penelitian menunjukkan bahwa meskipun regulasi telah menciptakan kerangka hukum yang komprehensif, efektivitasnya masih terkendala oleh keterlambatan pembentukan lembaga pengawas independen, keterbatasan sumber daya manusia dan teknis, serta rendahnya kesadaran masyarakat dan pelaku usaha terhadap perlindungan data pribadi. Dampak ekonomi dari lemahnya implementasi tercermin dalam menurunnya kepercayaan publik, meningkatnya risiko investasi, dan berkurangnya daya saing digital nasional. Keberhasilan perlindungan data pribadi harus dipandang sebagai prasyarat utama bagi keberlanjutan ekonomi digital Indonesia melalui kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam menciptakan ekosistem digital yang aman, transparan, dan berdaya saing.

Kata Kunci: Perlindungan Data Pribadi, Ekonomi Digital, Keamanan Siber, Investasi Digital, Kepercayaan Publik.

PENDAHULUAN

Perkembangan ekonomi digital Indonesia yang pesat membawa implikasi terhadap perlindungan data pribadi. Transformasi digital yang mengakselerasi berbagai sektor ekonomi, mulai dari perdagangan elektronik, layanan keuangan digital, hingga layanan publik berbasis daring, menciptakan volume data pribadi yang sangat besar (Zainuddin, et al., 2025). Data pribadi telah menjadi aset strategis dalam ekonomi digital, namun sekaligus meningkatkan risiko penyalahgunaan dan kebocoran data yang dapat menimbulkan kerugian ekonomi dan sosial yang signifikan (Alvember, & Asri, 2025).

Insiden kebocoran Pusat Data Nasional pada Juni 2024 menjadi momentum kritis yang mengekspos kelemahan fundamental sistem keamanan siber nasional. Serangan ransomware terhadap Pusat Data Nasional Sementara melumpuhkan lebih dari 210 instansi pemerintah, dengan data yang

terdampak tidak dapat dipulihkan. Peretas meminta tebusan senilai 8 juta dolar Amerika Serikat atau sekitar 131,6 miliar rupiah. Insiden ini mengganggu berbagai layanan publik penting termasuk sistem perpajakan, keimigrasian, dan pendidikan, serta menimbulkan kekhawatiran besar di kalangan masyarakat terkait keamanan data pribadi mereka (Adristi, & Ramadhani, 2024).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi disahkan pada 17 Oktober 2022 setelah melalui proses perumusan yang panjang sejak tahun 2006 (Rosadi, 2023). Regulasi ini mengatur secara komprehensif mengenai asas, jenis data pribadi, hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali dan prosesor data pribadi, transfer data pribadi, sanksi administratif, kelembagaan, kerja sama internasional, partisipasi masyarakat, penyelesaian sengketa, larangan, dan ketentuan pidana terkait perlindungan data pribadi (Salsabila, & Wiraguna, 2025).

Dalam beberapa tahun terakhir, percepatan transformasi digital di Indonesia telah membuka sekaligus memacu potensi ekonomi yang sangat besar, khususnya melalui sektor-sektor seperti perdagangan elektronik, layanan keuangan digital, dan platform layanan publik daring (Hapiz, et al. 2025). Kemunculan dan pertumbuhan ekosistem ekonomi digital tersebut juga secara otomatis meningkatkan nilai ekonomi dari data pribadi sebagai aset strategis, karena data menjadi input penting untuk analisis pasar, personalisasi layanan, efisiensi operasional, dan inovasi bisnis.

Lonjakan volume data pribadi yang dikelola di berbagai sektor juga berarti lonjakan risiko kebocoran yang bila tidak dikelola dengan baik akan berdampak langsung terhadap kerugian fiskal, meningkatnya biaya pemulihan, kerusakan reputasi perusahaan, bahkan menurunnya kepercayaan konsumen. Sebagai gambaran empiris berikut data jumlah akun yang mengalami kebocoran di Indonesia dalam beberapa tahun terakhir:

Tabel 1. Tren Kebocoran Data Pribadi di Indonesia

Tahun	Akun Bocor di Indonesia
Jan 2004–Jan 2024	156,8 juta akun per laporan Surfshark
2020	Sekitar 70 juta akun dari satu kasus besar di e-commerce Indonesia

Sumber: Surfshark (2025), Surfshark (2023)

Data tersebut menggambarkan skala ekonomi yang terpapar jika sistem perlindungan data tidak memadai biaya langsung maupun tidak langsung dapat menggerus keuntungan, menghambat investasi digital, dan memperlambat arus pertumbuhan ekonomi digital. Setelah pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan penerapan penuh sejak 17 Oktober 2024, Indonesia telah mengambil langkah hukum penting dalam menciptakan kerangka regulasi yang lebih kuat untuk melindungi data pribadi dan mendukung ekosistem digital yang sehat (Suzana, & Michael, 2024).

Dalam ekonomi adanya kepercayaan pengguna dan bisnis terhadap keamanan data menjadi salah satu variabel kritis dalam memacu volume transaksi digital, pangsa pasar fintech, dan adopsi layanan digital baru; tanpa perlindungan data yang kredibel, potensi tersebut bisa tertahan (Tsakila, et al., 2024). Efektivitas implementasi UU PDP dapat dilihat sebagai bagian tak terpisahkan dari strategi nasional untuk menjaga stabilitas dan pertumbuhan ekonomi digital secara berkelanjutan.

Tantangan implementasi masih cukup berat dan dengan implikasi ekonomi. Tingkat kebocoran data di Indonesia tergolong tinggi dalam skala global, yang menunjukkan bahwa lemahnya standar keamanan dan penerapan kebijakan dapat menggerus peluang ekonomi digital. Ketika organisasi publik maupun swasta mengalami insiden kebocoran, konsekuensinya potensi hilangnya transaksi, penurunan pangsa pasar, dan meningkatnya biaya kepatuhan dan pemulihan yang secara kolektif bisa menghambat kontribusi ekonomi sektor digital terhadap PDB (Prastyanti, 2025).

Ekosistem digital yang inklusif memerlukan regulasi, teknologi, dan kepercayaan publik-bisnis agar dapat menghasilkan multiplier effect yang signifikan (Pradono, & Pradhitasari, 2016). Ketika pengguna yakin bahwa data mereka dikelola dengan aman, mereka cenderung lebih aktif menggunakan layanan digital yang kemudian mendorong skala ekonomi, efisiensi industri, inovasi produk, dan ekspansi pasar baik domestik maupun lintas negara.

Penelitian ini bertujuan menganalisis efektivitas implementasi Undang-Undang Perlindungan Data Pribadi dalam mendukung stabilitas ekonomi digital Indonesia. Kajian akan mengidentifikasi tantangan implementasi regulasi, dampak kebocoran data terhadap ekonomi digital, serta merumuskan rekomendasi kebijakan untuk memperkuat ekosistem perlindungan data pribadi. Analisis ini penting

mengingat ekonomi digital Indonesia diproyeksikan terus tumbuh pesat dan memerlukan fondasi perlindungan data yang kuat untuk membangun kepercayaan publik dan mendorong transformasi digital yang berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode analisis data sekunder (Qomaruddin, & Sa'diyah, 2024). Data dikumpulkan dari berbagai sumber terpercaya meliputi peraturan perundang-undangan terkait perlindungan data pribadi, laporan resmi kementerian dan lembaga pemerintah, publikasi lembaga riset dan organisasi internasional, pemberitaan media massa terkait insiden kebocoran data, artikel jurnal ilmiah tentang perlindungan data dan keamanan siber, serta dokumen kebijakan dan panduan implementasi dari berbagai negara.

Analisis data dilakukan melalui beberapa tahapan sistematis (Dewi, et al. 2025). Pertama, mengidentifikasi dan mengkaji kerangka regulasi perlindungan data pribadi di Indonesia beserta aturan pelaksanaannya. Kedua, menganalisis kasus-kasus kebocoran data yang terjadi di Indonesia untuk mengidentifikasi pola, penyebab, dan dampaknya. Ketiga, mengevaluasi implementasi regulasi dengan mengidentifikasi tantangan dan hambatan yang dihadapi oleh pemangku kepentingan. Keempat, menganalisis dampak kebocoran data terhadap ekonomi digital Indonesia meliputi aspek kepercayaan, investasi, dan adopsi teknologi. Kelima, membandingkan praktik implementasi regulasi perlindungan data di Indonesia dengan praktik terbaik internasional untuk mengidentifikasi pembelajaran dan rekomendasi. Keenam, mensintesis temuan untuk merumuskan rekomendasi kebijakan yang dapat memperkuat efektivitas implementasi regulasi perlindungan data pribadi. Analisis dilakukan dengan mempertimbangkan konteks ekonomi digital Indonesia, karakteristik infrastruktur teknologi, kapasitas institusional, dan dinamika sosial budaya untuk menghasilkan rekomendasi yang implementatif dan kontekstual.

Keterbatasan penelitian ini meliputi penggunaan data sekunder yang tergantung pada ketersediaan dan kualitas data yang dipublikasikan. Beberapa informasi terkait implementasi regulasi dan dampak ekonomi mungkin tidak sepenuhnya terungkap karena sifatnya yang sensitif. Penelitian ini juga tidak melakukan survei atau wawancara mendalam dengan pemangku kepentingan karena keterbatasan waktu dan akses. Namun, pendekatan kualitatif deskriptif yang digunakan tetap dapat memberikan gambaran komprehensif tentang efektivitas implementasi regulasi perlindungan data pribadi dalam mendukung stabilitas ekonomi digital Indonesia

HASIL DAN PEMBAHASAN

Kondisi Kebocoran Data di Indonesia

Analisis terhadap kondisi kebocoran data di Indonesia menunjukkan situasi yang mengkhawatirkan dengan peningkatan frekuensi dan skala insiden. Berdasarkan data Kementerian Komunikasi dan Digital, jumlah kasus dugaan pelanggaran perlindungan data pribadi menunjukkan tren peningkatan dari tiga kasus pada tahun 2019 menjadi 21 kasus pada 2020, 20 kasus pada 2021, 35 kasus pada 2022, 40 kasus pada 2023, dan lima kasus hingga Mei 2024. Total 124 kasus yang ditangani selama periode tersebut, dimana 111 kasus merupakan kebocoran data pribadi, empat kasus pengungkapan kepada pihak tidak berwenang, dan tiga kasus pengumpulan data yang tidak relevan (Kompas. 2024).

Temuan mengkhawatirkan adalah mayoritas data yang bocor tidak melalui proses enkripsi. Dari 124 kasus yang ditangani, hanya dua kasus yang ditemukan mengumpulkan data pribadi melalui proses enkripsi, sementara mayoritas lainnya merupakan data yang tidak terenkripsi atau dalam kondisi terbuka (Kompas. 2024). Kondisi ini sangat berbahaya karena data yang bocor dapat langsung dibaca dan digunakan untuk tujuan kriminal. Analisis lebih lanjut menunjukkan bahwa mayoritas kebocoran data tidak terenkripsi cenderung berasal dari instansi pemerintah, mengindikasikan lemahnya standar keamanan data di sektor publik. Tabel berikut menunjukkan perkembangan kasus pelanggaran perlindungan data pribadi yang ditangani Kementerian Komunikasi dan Digital.

Tabel 2. Perkembangan Kasus Pelanggaran Perlindungan Data Pribadi 2019-2024

Tahun	Jumlah Kasus	Kebocoran Data	Persentase

2019	3	3	100%
2020	21	19	90,5%
2021	20	17	85%
2022	35	32	91,4%
2023	40	36	90%
2024 (hingga Mei)	5	4	80%
Total	124	111	89,5%

Kompas (2024)

Penyebab kebocoran data menunjukkan beberapa faktor fundamental. Pertama, lemahnya infrastruktur keamanan siber dengan sistem yang tidak diperbarui, konfigurasi keamanan yang salah, dan tidak adanya sistem pertahanan berlapis. Kedua, rendahnya kesadaran dan kompetensi keamanan data dengan kurangnya pelatihan, ketidaktahuan tentang praktik keamanan, dan kelalaian dalam pengelolaan data. Ketiga, keterbatasan sumber daya dengan anggaran keamanan siber yang terbatas, kurangnya tenaga ahli keamanan siber, dan prioritas rendah terhadap investasi keamanan. Keempat, lemahnya pengawasan dan akuntabilitas dengan tidak adanya audit keamanan berkala, kurangnya mekanisme deteksi dini, dan respons lambat terhadap insiden.

Tantangan Implementasi Perlindungan Data Pribadi pada Ekonomi Digital

Salah satu hambatan utama ekonomi berasal dari keterlambatan pembentukan lembaga pengawas independen yang dimandatkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, karena tanpa kehadiran lembaga yang efektif untuk mengawasi pelaksanaan kewajiban pengendali dan prosesor data, maka risiko regulasi menjadi hanya formalitas dan tidak menciptakan efek ekonomi yang optimal (Nasution, & Harmika, 2025).

Ketidakpastian kelembagaan ini menciptakan biaya penghambat investasi digital, karena pelaku usaha memerlukan kepastian regulasi dan pengawasan agar dapat mengalokasikan modal untuk teknologi perlindungan data tanpa khawatir mengenai eksposur sanksi yang tidak konsisten (Wibowo, 2024). Misalnya jika sebuah startup fintech menunda ekspansi ke layanan baru karena harus menunggu pedoman teknis lembaga pengawas, maka pertumbuhan pendapatan dan penciptaan lapangan kerja digital tertahan. Berikut ini data frekuensi pelaporan insiden kebocoran data di Indonesia yang dapat memperlihatkan potensi kerugian ekonominya.

Tabel 3. Jumlah Insiden Kebocoran Data Pribadi di Indonesia Tahun 2020–2025

Tahun	Jumlah Insiden Kebocoran Data
2023	154.080 akun terbobol di kuartal 4
2024 (Q3)	16.060.000 akun terbobol
Cumulatif 2020-Jan 2025	~114.090.000 akun terbobol

Sumber: Databoks (2025), Medium (2025)

Ketiadaan lembaga pengawas yang mapan mengakibatkan biaya kepatuhan yang lebih tinggi bagi pelaku usaha (karena harus mengantisipasi ketidakjelasan), sekaligus mengurangi insentif untuk berinovasi dalam ekonomi digital karena risiko regulatorium yang belum stabil. Dalam hal sosialisasi dan pemahaman pelaku usaha, kendala tersebut bukan hanya bersifat hukum tetapi juga berdampak langsung terhadap efisiensi ekonomi sektor digital, karena ketika usaha mikro, kecil dan menengah (UMKM) atau perusahaan rintisan (*startup*) tidak memahami kewajiban regulasi data pribadi maka mereka cenderung menunda atau bahkan menghindari adopsi teknologi baru yang seharusnya meningkatkan produktivitas (Purba, et al., 2025).

Keterbatasan sumber daya teknis dan sumber daya manusia dalam implementasi regulasi juga memiliki konsekuensi ekonomi yang nyata, karena investasi yang tinggi dalam infrastruktur keamanan data, sistem manajemen data, dan pelatihan tenaga SDM menghasilkan biaya awal (initial cost) yang besar jika tidak diimbangi dengan pendapatan tambahan atau efisiensi operasional, maka margin keuntungan sektor digital dapat tertekan (Latif, & Ali, 2025). Investasi tersebut pada akhirnya harus dipasukkan ke dalam model bisnis pelaku usaha, yang jika tidak optimal dapat menurunkan daya saing

dibandingkan dengan negara lain di kawasan yang memiliki biaya *compliance* lebih rendah. Untuk menegaskan skala risiko teknis tersebut, berikut data dari hasil monitoring instansi keamanan siber.

Tabel 4. Kasus Paparan (*Exposure*) Data Pribadi di Indonesia Tahun 2023–2024

Tahun	Data "*exposure*"
2023	1.674.185 eksposur data berdampak pada 429 stakeholder
2024	56.128.160 temuan data exposure berdampak 461 stakeholder

Sumber: Nurulita (2025)

Data di atas menunjukkan bahwa tanpa kompetensi yang memadai dan investasi yang cukup, organisasi tidak hanya menghadapi risiko regulasi tetapi juga kerugian nyata dari kebocoran data, seperti pemulihan kerugian, hilangnya kepercayaan pelanggan, atau potensi litigasi semua berpotensi menggerus pertumbuhan ekonomi digital. Maka dari itu, hambatan sumber daya ini bukan hanya isu teknis semata tetapi juga faktor ekonomi strategis yang harus diperhitungkan dalam kerangka pengembangan ekonomi digital nasional.

Rendahnya kesadaran masyarakat terhadap hak privasi data pribadi juga berimplikasi pada ekonomi digital, karena kepercayaan pengguna menjadi salah satu prasyarat penting bagi transaksi digital, pemanfaatan layanan berbasis data, dan terciptanya ekosistem bisnis yang aktif (Lisdayanti, & Padmanegara, 2024). Ketika masyarakat tidak memahami risiko atau hak-hak mereka sebagai subjek data, maka tingkat adopsi layanan digital berisiko stagnan atau menurun, yang dapat menurunkan potensi pendapatan bagi perusahaan dan menghambat multiplier effect ekonomi digital.

Implementasi Undang-Undang Perlindungan Data Pribadi menghadapi tantangan kompleks yang menghambat efektivitasnya. Tantangan pertama adalah keterlambatan pembentukan lembaga pengawas independen yang merupakan amanat krusial dalam regulasi. Hingga regulasi berlaku penuh pada Oktober 2024, lembaga pengawas belum terbentuk. Peraturan Presiden tentang pembentukan lembaga pengawas dan Peraturan Pemerintah sebagai pedoman teknis pelaksanaan masih dalam proses harmonisasi di Kementerian Hukum dan Hak Asasi Manusia. Keterlambatan ini menciptakan kekosongan institusional yang menghambat pengawasan, penegakan, dan memberikan ketidakpastian bagi pelaku usaha.

Tantangan kedua adalah kurangnya sosialisasi dan pemahaman pelaku usaha terhadap kewajiban dalam regulasi. Banyak organisasi, khususnya usaha mikro kecil dan menengah, belum memahami secara komprehensif kewajiban penunjukan pejabat pelindungan data, penyusunan kebijakan pengelolaan data, implementasi langkah pengamanan, dan dokumentasi kegiatan pemrosesan. Survei menunjukkan masih tingginya gap pemahaman antara ketentuan regulasi dengan praktik di lapangan. Kurangnya panduan teknis yang mudah dipahami dan praktis memperburuk situasi implementasi.

Tantangan ketiga adalah keterbatasan sumber daya teknis dan sumber daya manusia. Implementasi regulasi memerlukan investasi signifikan dalam infrastruktur keamanan, teknologi enkripsi, sistem manajemen data, dan pelatihan personel. Bagi organisasi dengan kapasitas terbatas, beban biaya compliance dapat menjadi hambatan. Kelangkaan profesional dengan kompetensi perlindungan data dan keamanan siber mempersulit organisasi dalam memenuhi kewajiban regulasi. Keterbatasan anggaran pemerintah untuk program edukasi dan fasilitasi implementasi juga menjadi kendala.

Tantangan keempat adalah rendahnya kesadaran masyarakat terhadap hak privasi data. Banyak masyarakat masih belum memahami pentingnya melindungi data pribadi, risiko penyalahgunaan data, dan hak-hak yang dimiliki sebagai subjek data. Budaya berbagi data secara sembarangan tanpa mempertimbangkan implikasi keamanan masih menjamur. Kurangnya pemahaman ini membuat masyarakat rentan menjadi korban kejahatan siber dan kurang kritis dalam mengevaluasi praktik pengelolaan data oleh organisasi.

Tantangan kelima adalah kompleksitas harmonisasi dengan regulasi sektoral existing. Banyak sektor seperti perbankan, telekomunikasi, kesehatan, memiliki regulasi khusus terkait pengelolaan data. Harmonisasi antara Undang-Undang Perlindungan Data Pribadi yang bersifat umum dengan regulasi sektoral yang khusus memerlukan kajian mendalam untuk memastikan tidak ada konflik atau kekosongan hukum. Tantangan keenam adalah lemahnya mekanisme penegakan hukum. Meskipun regulasi menetapkan sanksi berat, efektivitas penegakan masih dipertanyakan mengingat keterbatasan

kapasitas aparat, kompleksitas teknis bukti digital, dan belum adanya preseden kasus yang memberikan pembelajaran.

Dampak Kebocoran Data terhadap Ekonomi Digital

Analisis dampak kebocoran data terhadap ekonomi digital menunjukkan implikasi yang luas dan signifikan. Dampak pertama adalah erosi kepercayaan publik terhadap layanan digital. Insiden kebocoran data yang berulang dan berskala besar menciptakan persepsi negatif terhadap keamanan layanan digital Indonesia. Penelitian menunjukkan bahwa persepsi keamanan data yang rendah dapat menurunkan tingkat partisipasi masyarakat dalam ekonomi digital, mempengaruhi keputusan penggunaan layanan digital, dan menurunkan kepercayaan terhadap pemerintah dan institusi dalam menjaga data pribadi.

Dampak kedua adalah penurunan daya tarik investasi di sektor digital. Investor mempertimbangkan kematangan regulasi dan praktik perlindungan data dalam keputusan investasi. Negara dengan tingkat kebocoran data tinggi dan regulasi lemah dianggap berisiko tinggi. Hal ini dapat menghambat masuknya investasi asing langsung, mengurangi valuasi perusahaan digital, dan memperlambat pertumbuhan startup teknologi. Sektor ekonomi digital yang sangat bergantung pada kepercayaan dan keamanan data akan mengalami hambatan pertumbuhan signifikan.

Dampak ketiga adalah kerugian finansial langsung yang ditanggung korban dan organisasi. Korban kebocoran data mengalami kerugian melalui penipuan finansial, pencurian identitas, pembobolan rekening, dan biaya pemulihan dokumen. Organisasi yang mengalami kebocoran menanggung biaya investigasi insiden, pemulihan sistem, kompensasi korban, denda regulasi, biaya hukum, dan biaya pemulihan reputasi. Studi menunjukkan biaya rata-rata penanganan insiden kebocoran data sangat tinggi dan dapat mengancam kelangsungan bisnis organisasi kecil dan menengah.

Dampak keempat adalah hambatan transformasi digital nasional. Pemerintah mendorong transformasi digital di berbagai sektor untuk meningkatkan efisiensi dan kualitas layanan publik. Namun, insiden kebocoran data menciptakan resistensi masyarakat terhadap digitalisasi. Masyarakat menjadi ragu menggunakan layanan digital pemerintah seperti sistem perpajakan digital, layanan kependudukan digital, dan platform layanan publik lainnya. Hal ini menghambat pencapaian target transformasi digital nasional dan modernisasi birokrasi.

Dampak kelima adalah penurunan daya saing Indonesia di pasar digital global. Standar perlindungan data semakin menjadi pertimbangan dalam perdagangan digital internasional. Negara dan perusahaan dengan standar perlindungan data rendah dapat menghadapi hambatan akses pasar, kesulitan kemitraan dengan perusahaan multinasional, dan penurunan reputasi global. Hal ini dapat menghambat ekspor jasa digital Indonesia, mengurangi peluang kolaborasi teknologi, dan melemahkan posisi Indonesia dalam ekonomi digital regional dan global. Dampak agregat dari berbagai aspek ini menunjukkan bahwa kebocoran data bukan hanya isu teknis keamanan, tetapi merupakan ancaman serius terhadap stabilitas dan pertumbuhan ekonomi digital Indonesia.

Evaluasi efektivitas Undang-Undang Perlindungan Data Pribadi dalam fase awal implementasi menunjukkan hasil yang beragam. Dari sisi positif, regulasi telah memberikan kerangka hukum komprehensif yang mengatur perlindungan data pribadi secara holistik. Keberadaan regulasi menciptakan dasar hukum yang jelas tentang hak dan kewajiban dalam pengelolaan data pribadi, memberikan kepastian hukum bagi pelaku usaha, dan menjadi fondasi untuk harmonisasi regulasi sektoral. Ancaman sanksi yang berat berpotensi memberikan efek jera bagi pelanggar dan mendorong organisasi untuk meningkatkan standar perlindungan data.

Regulasi juga telah meningkatkan kesadaran tentang pentingnya perlindungan data pribadi. Pemberitaan media tentang regulasi dan insiden kebocoran data meningkatkan diskusi publik tentang privasi dan keamanan data. Beberapa organisasi besar telah mulai mengambil langkah proaktif dengan menunjuk pejabat pelindungan data, menyusun kebijakan pengelolaan data, dan meningkatkan investasi dalam keamanan siber. Program sosialisasi yang dilakukan berbagai kementerian dan lembaga mulai meningkatkan pemahaman pelaku usaha tentang kewajiban regulasi.

Namun, efektivitas regulasi masih terhambat oleh berbagai kendala implementasi. Keterlambatan pembentukan lembaga pengawas menciptakan kekosongan institusional yang menghambat fungsi pengawasan, penegakan, dan penanganan pengaduan. Tanpa lembaga pengawas yang berfungsi, mekanisme penegakan hukum tidak dapat berjalan optimal. Kurangnya aturan teknis pelaksanaan

membuat organisasi kesulitan menerjemahkan ketentuan regulasi ke dalam praktik operasional. Ketidakpastian tentang standar compliance yang diterima menciptakan kebingungan di kalangan pelaku usaha.

Insiden kebocoran data yang terus terjadi bahkan setelah regulasi berlaku menunjukkan bahwa keberadaan regulasi saja tidak cukup tanpa implementasi efektif. Kebocoran Pusat Data Nasional pada Juni 2024, beberapa bulan sebelum regulasi berlaku penuh, mengekspos bahwa infrastruktur keamanan siber nasional masih sangat lemah. Hal ini menunjukkan kesenjangan besar antara ketentuan normatif dalam regulasi dengan realitas praktik keamanan data di lapangan. Transformasi dari regulasi ke implementasi praktis memerlukan waktu, sumber daya, dan komitmen yang konsisten.

Perbandingan dengan implementasi regulasi perlindungan data di negara lain memberikan pembelajaran penting. Regulasi seperti General Data Protection Regulation di Uni Eropa menunjukkan bahwa efektivitas regulasi memerlukan beberapa elemen kunci yaitu lembaga pengawas yang independen dan berwenang, panduan teknis yang komprehensif dan praktis, program edukasi dan sosialisasi yang masif, penegakan hukum yang konsisten dengan preseden kasus yang jelas, dan kolaborasi erat antara regulator, industri, dan masyarakat sipil. Indonesia perlu mempercepat pemenuhan elemen-elemen ini untuk meningkatkan efektivitas regulasi perlindungan data pribadi.

KESIMPULAN

Perlindungan data pribadi sangat berkolerasi dengan stabilitas ekonomi digital, terutama dalam membangun kepercayaan konsumen, meningkatkan daya tarik investasi, serta memperluas partisipasi masyarakat dalam transaksi digital. Berbagai tantangan implementasi seperti keterlambatan pembentukan lembaga pengawas, lemahnya pemahaman pelaku usaha, serta minimnya sumber daya teknis dan manusia masih menjadi hambatan utama dalam penerapan regulasi ini. Kondisi tersebut menunjukkan perlunya percepatan pembentukan institusi pengawas dan peningkatan kapasitas nasional agar perlindungan data pribadi dapat benar-benar menjadi fondasi bagi pertumbuhan ekonomi digital yang inklusif dan berdaya saing.

Kebocoran data terbukti membawa dampak yang menggerus kepercayaan publik dan menimbulkan kerugian finansial signifikan baik bagi individu, pelaku usaha, maupun negara. Ketidakamanan data berimplikasi pada penurunan minat investasi digital, berkurangnya nilai pasar perusahaan teknologi, dan terhambatnya transformasi digital nasional. Implementasi perlindungan data pribadi yang efektif harus dipandang sebagai investasi ekonomi jangka panjang, bukan sekadar kepatuhan administratif. Diperlukan sinergi antara pemerintah, pelaku industri, dan masyarakat untuk menciptakan ekosistem digital yang aman, transparan, dan berkeadilan. Apabila kebijakan ini dijalankan secara konsisten dan disertai penguatan kapasitas teknis, maka Undang-Undang Perlindungan Data Pribadi dapat berfungsi sebagai pilar utama dalam menjaga stabilitas, kepercayaan, dan pertumbuhan ekonomi digital Indonesia di masa mendatang.

DAFTAR PUSTAKA

Adristi, F. I., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *2*(6), 196-212.

Alvember, M., & Asri, D. P. B. (2025). Analisis Keamanan Data Pribadi Konsumen terhadap Regulasi Pencantuman Nomor Induk Kependudukan untuk Registrasi Nomor Telepon. *Arus Jurnal Sosial dan Humaniora*, *5*(2), 3017-3026. https://doi.org/10.57250/ajsh.v5i2.1590.

Databoks. (2025). "Indonesia's Data Breach Trend Decreases by the End of 2024", tersedia di https://databoks.katadata.co.id/en/technology-telecommunications/statistics/67a871ef10fcb/indonesias-data-breach-trend-decreases-by-the-end-of-2024, diakses pada 27 Oktober 2025.

Dewi, A. P., Erlansyah, A. C., Dwi, S. C., Berliana, W. F., Putri, Z. K., & Supriyadi, T. (2025). Model Proses Dan Tahapan Sistematis Dalam Intervensi Sosial: Pendekatan Teori Dan Praktik. *Humanitis: Jurnal Homaniora, Sosial dan Bisnis*, *3*(1), 1-12.

Hapiz, M., Septia, L. P., Aprilianti, D., Aprilianto, D., Maulida, I., Muhammad, F., ... & Herdiana, D. (2025). Analisis Kebijakan Pengembangan UMKM Digital di Indonesia: Tantangan dan

Peluang. *Madani: Jurnal Ilmiah Multidisiplin*, *3*(5), 36-44. https://doi.org/10.5281/zenodo.15538100.

Kompas. (2024). "Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024", tersedia di https://www.kompas.id/artikel/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024, diakses pada 27 Oktober 2025.

Latif, D. P., & Ali, H. (2025). Pengaruh Pengambilan Keputusan, Investasi Teknologi Informasi dan Pengembangan SDM terhadap Efisiensi Operasional. *Jurnal Komunikasi dan Ilmu Sosial*, *3*(1), 1-10. https://doi.org/10.38035/jkis.v3i1.1724.

Lisdayanti, A., & Padmanegara, O. H. (2024). Peran teknologi blockchain dalam meningkatkan kepercayaan konsumen dan keamanan data privasi pada platform e-commerce di Indonesia. *Jurnal Manajemen Bisnis dan Keuangan*, *5*(2), 347-361. https://doi.org/10.51805/jmbk.v5i2.245.

Medium. (2025). "A Reflection on Cybersecurity Industry Trends in Indonesia", tersedia di https://medium.com/%40kesha.mr77/securing-the-digital-frontier-reflections-on-cybersecurity-industry-trends-in-indonesia-42b7dfa5273a, diakses pada 27 Oktober 2025.

Nasution, E. R., & Harmika, Z. (2025). Perlindungan Hukum Terhadap Nasabah Bank Yang Mengalami Kebocoran Data Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022. *Innovative: Journal Of Social Science Research*, *5*(4), 11373-11384. https://doi.org/10.31004/innovative.v5i4.20892.

Nurulita, S. (2025). Political Will of The Indonesian Government in Addressing Data Leakage and Cybersecurity in the Era of Digital Transformation. *JHSS (Journal of Humanities and Social Studies)*, *9*(1), 028-038. https://doi.org/10.33751/jhss.v9i1.33.

Pradono, P., & Pradhitasari, H. (2016). Manfaat investasi pembangunan jalan tol bandung intra urban dari perspektif makro. *Tataloka*, *13*(2), 82-95. https://doi.org/10.14710/tataloka.13.2.82-95.

Prastyanti, R. A. (2025). *Monograf Perlindungan Data Pribadi Konsumen Pengguna Transaksi Elektronik*. Penerbit NEM.

Purba, D. S., Permatasari, P. D., Tanjung, N., Rahayu, P., Fitriani, R., & Wulandari, S. (2025). Analisis Perkembangan Ekonomi Digital dalam Meningkatkan Pertumbuhan Ekonomi di Indonesia. *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, *10*(1). https://doi.org/10.30651/jms.v10i1.25367.

Qomaruddin, Q., & Sa'diyah, H. (2024). Kajian teoritis tentang teknik analisis data dalam penelitian kualitatif: Perspektif Spradley, Miles dan Huberman. *Journal of Management, Accounting, and Administration*, *1*(2), 77-84. https://doi.org/10.52620/jomaa.v1i2.93.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2), 145-157. https://doi.org/10.62383/konsensus.v2i2.736.

Surfshark. (2023). "Holiday shopping alert: retail breaches exposed", tersedia di https://surfshark.com/research/chart/retail-breaches-exposed?srsltid=AfmBOorXutRnnYJizMRxExCa9sdxEeLUrSSiV1lNOov6WCzuE-qlwBQJ, diakses pada 27 Oktober 2025.

Surfshark. (2025). "Global data breach statistics", tersedia di https://surfshark.com/research/data-breach-monitoring?srsltid=AfmBOoqmLJ8JMwku8YFd6BQ7VHCv5VQn5KtOREz96rzL9XXDiHu1vN-c, diakses pada 27 Oktober 2025.

Suzana, M. V., & Michael, T. (2024). Pengaturan Hukum Penyalahgunaan Data Pribadi Penyandang Disabilitas Fisik di Era Digital. *Media Hukum Indonesia (MHI)*, *2*(4). https://doi.org/10.5281/zenodo.14176415.

Tsakila, N. F., Wirahadi, M. A., Fadilah, A. A., Simanjuntak, H., & Siswajanty, F. (2024). Analisis dampak fintech terhadap kinerja dan inovasi perbankan di era ekonomi digital. *Indonesian Journal of Law and Justice*, *1*(4), 11-11. https://doi.org/10.47134/ijlj.v1i4.2787.

Wibowo, M., Fatimah, E. N., & Wibowo, A. A. P. (2024). Pengawasan Persaingan Usaha dan Kepastian Hukum: Tantangan dan Solusi. *Journal of Knowledge and Collaboration*, *1*(3), 116-122. https://doi.org/10.59613/p95e8z22.

Zainuddin, Z., Sari, M., & Puspita, A. (2025). Analisis Dampak Ekonomi Digital Terhadap Masyarakat Dan Pertumbuhan Ekonomi Di Indonesia. *Journal of Economics Development Research*, *1*(2), 55-60. https://doi.org/10.71094/joeder.v1i2.112.