Jurnal Enterprise dan Tata Kelola Perusahaan: Manajemen dan Akuntansi
Volume:2, Nomor: 1, (2026), Juni: 127 - 137
Link Publish: https://ejournal.lppnusantara.com/index.php/jetp/article/view/902
E-ISSN: 3124-002X; DOI: https://doi.org/10.65244/jetp.v2i1.902

IMPLEMENTASI DATA PRIVACY BERBASIS ANONIMISASI DALAM DATABASE TRANSAKSI UNTUK MENJAGA KERAHASIAAN KONSUMEN DIGITAL

M Riyadh Riziq [1], Muhammad Irwan Padli Nasution [2]
Universitas Islam Negeri Sumatera Utara
Corresponding Author: riyadhriziq28@gmail.com , irwannst@uinsu.ac.id

Info Artikel
Submitted: *01 Mei 2026*
Revised : *02 Juni 2026*
Accepted: *12 Juni 2026*
Published: *25 Juni 2026*

Keywords: *data anonymization, digital privacy, transaction database, k-anonymity, differential privacy, PDP Law*

Abstract
Consumer data privacy has become a critical issue in the digital era as more and more transactions are conducted through online platforms. Storing large amounts of transaction data increases the risk of personal information leaks, both due to cyberattacks and data mismanagement. This article discusses the use of data anonymization techniques as a privacy protection measure in transaction databases, focusing on k-anonymity, l-diversity, and differential privacy. The study employed a systematic literature review, analyzing various scientific sources related to data anonymization and digital privacy security. The results show that each technique has advantages and disadvantages. K-anonymity can disguise user identity but still has weaknesses for sensitive data. L-diversity provides better protection by increasing the variety of sensitive attributes, while differential privacy offers stronger privacy protection by adding noise to the data. The application of anonymization techniques supported by regulations such as the GDPR and the Indonesian Privacy and Data Protection Law can help improve consumer data security without reducing the data's usefulness for analysis. This research is expected to serve as a reference for system developers, data analysts, and policymakers in developing privacy protection systems in the digital era.

Kata Kunci: *anonimisasi data, privasi digital, database transaksi, k-anonymity, differential privacy,UU PDP*

Abstrak
Privasi data konsumen menjadi isu penting di era digital karena semakin banyak transaksi dilakukan melalui platform online. Penyimpanan data transaksi dalam jumlah besar meningkatkan risiko kebocoran informasi pribadi, baik akibat serangan siber maupun kesalahan pengelolaan data. Artikel ini membahas penggunaan teknik anonimisasi data sebagai upaya perlindungan privasi pada database transaksi, dengan fokus pada metode k-anonymity, l-diversity, dan differential privacy. Penelitian menggunakan metode kajian literatur sistematis dengan menganalisis berbagai sumber ilmiah terkait anonimisasi data dan keamanan privasi digital. Hasil penelitian menunjukkan bahwa setiap teknik memiliki kelebihan dan kekurangan. K-anonymity mampu menyamarkan identitas pengguna, tetapi masih memiliki kelemahan pada data sensitif. L-diversity memberikan perlindungan lebih baik dengan menambah variasi atribut sensitif, sedangkan differential privacy menawarkan perlindungan privasi yang lebih kuat melalui penambahan noise pada data. Penerapan teknik anonimisasi yang didukung regulasi seperti GDPR dan UU PDP Indonesia dapat membantu meningkatkan keamanan data konsumen tanpa mengurangi manfaat data untuk analisis. Penelitian ini diharapkan dapat menjadi referensi bagi pengembang sistem, analis data, dan pembuat kebijakan dalam membangun sistem perlindungan privasi di era digital.

PENDAHULUAN

Dalam lanskap ekonomi digital yang berkembang pesat, setiap interaksi pengguna dengan platform daring mulai dari pembelian produk, pemrosesan pembayaran, hingga pencatatan riwayat navigasi menghasilkan jejak data yang sangat berharga. Data-data ini tidak sekadar angka, mereka merupakan representasi digital dari perilaku, preferensi, dan bahkan kondisi finansial seseorang. Sayangnya, nilai ekonomis yang tinggi dari data tersebut menjadikannya target utama bagi berbagai ancaman, baik dari pelaku kejahatan siber eksternal maupun dari praktik pengelolaan data internal yang kurang bertanggung jawab.

Sejumlah insiden pelanggaran data berskala besar telah membuktikan betapa rentannya informasi pribadi konsumen ketika tidak dikelola dengan mekanisme perlindungan yang memadai. Laporan dari IBM Security (2023) mencatat bahwa rata-rata biaya pelanggaran data secara global mencapai USD 4,45 juta per insiden, angka tertinggi sepanjang sejarah pemantauan tersebut. Di Indonesia, kasus kebocoran data seperti yang dialami oleh sejumlah lembaga keuangan dan platform *e-commerce* pada periode 2021–2023 memperkuat urgensi penerapan kerangka perlindungan data yang komprehensif (Kementerian Komunikasi dan Informatika RI, 2022). Respons regulatif pun mulai menguat: Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam tata kelola data nasional, mewajibkan setiap pengendali data untuk menerapkan langkah-langkah teknis dan organisasional yang proporsional dalam melindungi data pribadi yang diolahnya.

Di tengah berbagai pendekatan teknis yang tersedia, mulai dari enkripsi, pseudonimisasi, hingga kontrol akses berbasis peran, anonimisasi data menonjol sebagai solusi yang tidak hanya menjaga kerahasiaan informasi, tetapi juga tetap memungkinkan pemanfaatan data untuk keperluan analisis, riset, dan pengambilan keputusan bisnis. Teknik-teknik seperti *k-anonymity* (Sweeney, 2002), *l-diversity*, dan *differential privacy* (Dwork, 2006) telah berkembang menjadi fondasi ilmiah yang kuat dalam domain privasi data. Akan tetapi, penerapannya pada konteks spesifik database transaksi masih memerlukan kajian yang lebih mendalam, terutama dalam menyeimbangkan antara kekuatan proteksi privasi dan fungsionalitas data yang harus dipertahankan.

Celah penelitian (research gap) yang mendasari artikel ini terletak pada minimnya kajian yang secara khusus mengintegrasikan perspektif teknis anonimisasi dengan kerangka

regulatif kontekstual Indonesia, khususnya dalam kaitannya dengan database transaksi digital. Sebagian besar literatur yang ada berfokus pada anonimisasi data rekam medis atau data sensus, sementara karakteristik unik data transaksi seperti granularitas tinggi, volume besar, dan kebutuhan query real-time, menuntut pendekatan yang lebih terdiferensiasi.

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk: (1) menelaah prinsip-prinsip dasar dan mekanisme kerja teknik anonimisasi data yang relevan untuk database transaksi, (2) menganalisis efektivitas komparatif berbagai pendekatan anonimisasi dari sisi perlindungan privasi maupun utilitas data, (3) mengidentifikasi tantangan implementasi dan merekomendasikan kerangka penerapan yang praktis dan sesuai dengan regulasi yang berlaku di Indonesia.

TINJAUAN PUSTAKA

2.1 Konsep Privasi Data dan Anonimisasi

Privasi data, dalam pengertian ilmu komputer dan hukum informasi, merujuk pada hak individu untuk mengendalikan bagaimana informasi pribadi mereka dikumpulkan, diproses, dan didistribusikan (Acquisti et al., 2020). Dalam konteks sistem informasi modern, privasi data tidak lagi dapat direduksi menjadi sekadar mekanisme teknis, ia merupakan nilai fundamental yang menyentuh dimensi etika, hukum, dan kepercayaan publik. Voigt dan Von dem Bussche (2021) berargumen bahwa kepatuhan terhadap regulasi privasi semata tidak cukup, organisasi perlu mengadopsi pendekatan *privacy by design*, di mana perlindungan privasi tertanam sejak tahap perancangan arsitektur sistem, bukan sebagai tambalan di akhir.

Anonimisasi data didefinisikan sebagai proses memodifikasi kumpulan data sedemikian rupa sehingga individu yang menjadi subjek data tidak dapat lagi diidentifikasi, baik secara langsung maupun tidak langsung, oleh pihak mana pun yang memiliki akses terhadap data tersebut (European Data Protection Board, 2022).

2.2 Teknik-Teknik Anonimisasi Data

***K-Anonymity*.** Diperkenalkan oleh Latanya Sweeney pada tahun 2002. Teknik ini bertujuan membuat setiap data dalam dataset tidak bisa dibedakan dari minimal beberapa data lainnya berdasarkan atribut tertentu, seperti kode pos, tanggal lahir, dan jenis kelamin. Atribut tersebut disebut quasi-identifier karena jika digabungkan dapat digunakan untuk mengetahui identitas seseorang. Cara kerja teknik ini dilakukan dengan generalisasi, yaitu mengganti data

yang terlalu spesifik menjadi lebih umum, serta supresi, yaitu menghapus data yang tidak memenuhi syarat keamanan.

L-Diversity. *L-diversity* merupakan pengembangan dari k-anonymity untuk mengatasi kelemahannya. Pada *k-anonymity*, data masih bisa bocor jika dalam satu kelompok semua orang memiliki atribut sensitif yang sama. Oleh karena itu, *l-diversity* mengharuskan setiap kelompok memiliki beberapa variasi nilai atribut sensitif agar identitas pengguna lebih terlindungi. Cao dan Yoshikawa (2020) juga mengembangkan personalized *l-diversity*, yaitu metode yang dapat memberikan tingkat perlindungan berbeda sesuai risiko masing-masing pengguna. Pendekatan ini cocok digunakan pada database e-commerce yang memiliki banyak jenis pengguna.

Differential Privacy. *Differential privacy* (DP) diperkenalkan oleh Cynthia Dwork pada tahun 2006 dan dianggap sebagai salah satu teknik perlindungan privasi yang paling kuat. Teknik ini bekerja dengan menambahkan gangguan acak (noise) pada data sehingga informasi pribadi pengguna tidak mudah diketahui. Dalam DP terdapat parameter epsilon (ε) yang menentukan tingkat privasi: semakin kecil nilai epsilon, maka privasi semakin kuat tetapi akurasi data menjadi lebih rendah. Apple dan Google telah menggunakan teknik ini dalam sistem pengumpulan data mereka untuk melindungi privasi jutaan pengguna (Tang et al., 2022). Namun, Desfontaines dan Pejó (2020) menjelaskan bahwa dalam praktiknya nilai epsilon sering dibuat terlalu besar sehingga perlindungan privasinya menjadi kurang maksimal.

2.3 Regulasi Privasi Data: GDPR dan UU PDP Indonesia

Regulasi Perlindungan Data Umum Eropa atau *General Data Protection Regulation* (GDPR) yang berlaku sejak Mei 2018 telah menjadi standar de facto global dalam tata kelola data pribadi. Regulasi ini memperkenalkan prinsip-prinsip kunci seperti pembatasan tujuan (*purpose limitation*), minimalisasi data (*data minimization*), dan akuntabilitas, yang semuanya berimplikasi langsung pada bagaimana data transaksi harus dikelola dan dianonimisasi (Voigt & Von dem Bussche, 2021). Di sisi lain, Indonesia dengan UU PDP No. 27 Tahun 2022 mengadopsi prinsip-prinsip serupa dengan nuansa lokal, termasuk kewajiban pengendali data untuk menghapus data pribadi setelah masa retensi berakhir dan melaporkan pelanggaran data kepada otoritas dalam waktu 14 hari (Kementerian Komunikasi dan Informatika RI, 2022). Perpaduan antara persyaratan regulatif ini dengan implementasi teknis anonimisasi menciptakan sebuah kerangka perlindungan berlapis yang ideal untuk sistem database transaksi.

2.4 Penelitian Terdahulu

Fung et al. (2020) melakukan studi komprehensif tentang anonimisasi data dalam lingkungan *big data*, menyimpulkan bahwa teknik tradisional seperti k-anonymity menghadapi tantangan serius dalam hal skalabilitas ketika berhadapan dengan dataset bervolume besar dan berdimensi tinggi. Mereka merekomendasikan pendekatan hibrid yang mengombinasikan teknik anonimisasi berbasis partisi dengan mekanisme DP untuk mencapai keseimbangan yang lebih baik. Sementara itu, Domingo-Ferrer et al. (2021) mengeksplorasi penerapan anonimisasi dalam konteks *federated learning*, menunjukkan bahwa privasi data dapat dijaga bahkan ketika model machine learning dilatih secara kolaboratif tanpa perlu memusatkan data mentah di satu lokasi, sebuah paradigma yang semakin relevan dalam ekosistem fintech dan e-commerce. Di tingkat regional Asia Tenggara, penelitian oleh Noor et al. (2022) mengkaji kesiapan implementasi privasi data di sektor perbankan digital Indonesia dan Malaysia, menemukan bahwa meskipun kesadaran regulatif meningkat, kapasitas teknis untuk mengimplementasikan anonimisasi yang canggih masih menjadi hambatan signifikan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode Systematic Literature Review (SLR) yang dipandu oleh kerangka PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Metode ini dipilih karena penelitian berfokus pada pengumpulan, penelaahan, dan analisis berbagai sumber literatur yang telah ada sebelumnya. Dengan menggunakan SLR, peneliti dapat menyusun dan membandingkan hasil penelitian terdahulu secara sistematis sehingga diperoleh pemahaman yang lebih mendalam mengenai topik yang diteliti. Pendekatan ini tidak bertujuan menghasilkan data empiris baru melalui eksperimen, melainkan melakukan sintesis dan analisis kritis terhadap pengetahuan yang telah terdokumentasi dalam berbagai jurnal, artikel, maupun penelitian sebelumnya.

HASIL DAN PEMBAHASAN

4.1 Karakteristik Data Transaksi dan Implikasinya terhadap Privasi

Database transaksi digital memiliki karakteristik khusus yang membuatnya berbeda dari jenis data lainnya dan berpengaruh terhadap privasi pengguna. Data transaksi biasanya bersifat longitudinal, yaitu merekam aktivitas pengguna yang sama dalam jangka waktu yang panjang. Karena itu, meskipun identitas langsung seperti nama telah dihapus, pola perilaku seseorang masih dapat dikenali melalui riwayat transaksinya. Selain itu, data transaksi juga

mengandung banyak atribut seperti waktu transaksi, nilai pembelian, jenis produk, dan lokasi geografis yang dapat digunakan untuk mempersempit identitas seseorang. Penelitian bahkan menunjukkan bahwa hanya dengan beberapa data transaksi, identitas pengguna dalam dataset yang telah dianonimkan masih dapat diketahui kembali (Mivule, 2021).

Di sisi lain, database transaksi sangat penting untuk kebutuhan analisis, seperti sistem rekomendasi produk, deteksi penipuan, analisis tren pasar, dan personalisasi layanan. Semua kebutuhan tersebut memerlukan data yang detail agar hasil analisis lebih akurat. Namun, semakin kuat teknik anonimisasi yang diterapkan untuk melindungi privasi pengguna, maka kualitas dan kegunaan data untuk analisis juga dapat menurun. Kondisi ini dikenal sebagai privacy-utility trade-off, yaitu dilema antara menjaga privasi pengguna dan mempertahankan manfaat data untuk kebutuhan analitik (Mivule, 2021).

4.2 Analisis Komparatif Teknik Anonimisasi untuk Database Transaksi

Analisis dari berbagai penelitian menunjukkan bahwa tidak ada satu teknik anonimisasi yang paling sempurna untuk semua jenis database transaksi. Setiap teknik memiliki kelebihan dan kekurangan yang harus disesuaikan dengan kebutuhan penggunaan data.

Teknik k-anonymity cukup mudah diterapkan dan hasilnya juga mudah dipahami, sehingga sering digunakan oleh pengembang database. Namun, pada data transaksi yang sangat detail, seperti waktu transaksi hingga hitungan detik dan nilai transaksi yang spesifik, teknik ini membutuhkan nilai k yang sangat besar agar data benar-benar aman. Akibatnya, banyak informasi penting harus digeneralisasi sehingga ketelitian data menjadi berkurang. Selain itu, teknik ini juga masih rentan terhadap composition attacks, yaitu serangan yang dilakukan dengan menggabungkan beberapa versi dataset anonim untuk menemukan kembali identitas pengguna (Sánchez et al., 2021).

Teknik l-diversity dan variannya yaitu t-closeness dianggap lebih kuat dalam melindungi data sensitif. Teknik ini menjaga agar distribusi data sensitif dalam suatu kelompok tetap mirip dengan distribusi data secara keseluruhan. Penelitian Cao dan Yoshikawa (2020) menunjukkan bahwa penggunaan t-closeness pada data transaksi kartu kredit mampu menurunkan risiko identifikasi ulang hingga di bawah 5%, sementara akurasi sistem deteksi penipuan masih tetap tinggi, yaitu sekitar 87% dari performa awal. Meskipun demikian, teknik ini memiliki kelemahan berupa proses komputasi yang lebih rumit, terutama jika dataset memiliki banyak atribut.

Sementara itu, differential privacy dianggap sebagai teknik yang paling kuat dalam memberikan perlindungan privasi karena menggunakan model matematika yang ketat. Teknik ini bekerja dengan menambahkan noise atau gangguan acak pada hasil data sehingga informasi individu tidak dapat diketahui secara langsung. Contohnya, perusahaan dapat mempublikasikan total penjualan tanpa membuka data transaksi setiap pengguna. Tang et al. (2022) menjelaskan bahwa Apple menggunakan teknik ini dalam sistem RAPPOR untuk mengumpulkan data penggunaan emoji tanpa melanggar privasi pengguna. Namun, menurut Desfontaines dan Pejó (2020), nilai parameter privasi (epsilon) yang digunakan sering kali tidak dijelaskan secara terbuka kepada pengguna, sehingga perlindungan privasinya bisa saja tidak sekuat yang diperkirakan.

4.3 Kerangka Implementasi Anonimisasi untuk Database Transaksi

Berdasarkan sintesis literatur, artikel ini mengusulkan kerangka implementasi berlapis (layered implementation framework) yang terdiri dari empat tahap terintegrasi:

1. Klasifikasi dan Pemetaan Data (Data Classification & Mapping)

Langkah pertama dan paling fundamental adalah mengidentifikasi dan mengklasifikasikan seluruh atribut dalam database transaksi ke dalam tiga kategori: identifier langsung (nama, nomor identitas, alamat email), quasi-identifier (tanggal transaksi, nilai nominal, kode pos, kategori pembelian), dan atribut sensitif (status finansial, riwayat kredit, preferensi produk yang bersifat personal). Proses ini membutuhkan kolaborasi antara tim teknis, unit privasi, dan pemahaman mendalam tentang konteks bisnis. Pemetaan yang akurat adalah prasyarat mutlak, kesalahan pada tahap ini akan merusak seluruh rantai proteksi selanjutnya (Domingo-Ferrer et al., 2021).

2. Pemilihan dan Kalibrasi Teknik Anonimisasi

Pemilihan teknik harus disesuaikan dengan tujuan penggunaan data pasca-anonimisasi. Untuk keperluan analisis internal agregat, differential privacy dengan epsilon yang dikalibrasi terhadap sensitivitas kueri adalah pilihan yang tepat. Untuk dataset yang akan dibagikan ke pihak ketiga atau dipublikasikan, kombinasi k-anonymity dan l-diversity dengan parameter yang ditentukan berdasarkan analisis risiko re-identifikasi menjadi lebih relevan. Fung et al. (2020) merekomendasikan penggunaan *privacy risk score*, metrik komposit yang menggabungkan probabilitas re-identifikasi, sensitivitas atribut, dan potensi dampak kebocoran sebagai dasar penetapan parameter anonimisasi.

3. Pengujian dan Validasi

Sebelum deployment, dataset yang telah dianonimisasi harus melalui serangkaian uji keamanan, termasuk simulasi serangan re-identifikasi (*adversarial testing*), pengukuran *information loss* menggunakan metrik seperti Normalized Certainty Penalty (NCP) atau Average Equivalence Class Size (AECS), dan pengujian utilitas dengan membandingkan hasil analitik dari data asli versus data yang dianonimisasi. Mivule (2021) menekankan pentingnya mendokumentasikan seluruh proses pengujian ini sebagai bagian dari jejak audit (*audit trail*) yang diperlukan untuk demonstrasi kepatuhan regulasi.

4. Tata Kelola dan Pemantauan Berkelanjutan

Anonimisasi bukan aktivitas satu kali. Seiring evolusi teknologi, metode re-identifikasi baru terus berkembang, sehingga proteksi yang memadai hari ini mungkin tidak mencukupi esok hari. Organisasi perlu membangun mekanisme pemantauan risiko privasi yang berkelanjutan, melakukan re-evaluasi teknik anonimisasi secara periodik, dan memastikan seluruh proses berjalan dalam kerangka tata kelola yang konsisten dengan UU PDP dan regulasi sektoral yang relevan (Kementerian Komunikasi dan Informatika RI, 2022).

4.4 Tantangan Implementasi dan Pertimbangan Praktis

Penerapan teknik anonimisasi dalam dunia nyata memiliki beberapa tantangan yang cukup besar. Pertama, semakin banyak atribut atau informasi dalam data transaksi, maka semakin sulit membuat data menjadi anonim tanpa mengurangi kualitas data secara berlebihan. Kondisi ini disebut curse of dimensionality. Karena itu, diperlukan teknik untuk menyederhanakan data terlebih dahulu sebelum proses anonimisasi dilakukan (Fung et al., 2020).

Kedua, terdapat konflik antara anonimisasi dan kebutuhan audit data. Dalam aturan seperti Anti-Money Laundering (AML) dan Counter Terrorism Financing (CTF), data transaksi harus tetap dapat diperiksa secara lengkap untuk kebutuhan pengawasan dan investigasi. Hal ini bertentangan dengan prinsip anonimisasi yang bertujuan menyembunyikan identitas pengguna secara permanen. Oleh sebab itu, solusi yang banyak digunakan adalah memisahkan penyimpanan data: data asli yang terenkripsi disimpan dengan akses sangat terbatas, sedangkan data yang sudah dianonimkan digunakan untuk analisis dan pelaporan umum (Graef et al., 2021).

Ketiga, penerapan teknik modern seperti differential privacy membutuhkan tenaga ahli yang memahami statistik dan kriptografi. Namun, kemampuan tersebut belum banyak dimiliki oleh perusahaan teknologi. Noor et al. (2022) menemukan bahwa sekitar 67% perusahaan

fintech di Indonesia belum memiliki tenaga khusus yang memahami privasi data berbasis komputasi. Hal ini menunjukkan bahwa pelatihan dan kerja sama antara dunia akademik dan industri sangat dibutuhkan agar perlindungan data dapat diterapkan dengan lebih baik.

KESIMPULAN DAN SARAN

Kajian literatur yang dilakukan dalam artikel ini membawa pada beberapa kesimpulan substantif. Pertama, anonimisasi data berbasis teknik yang mapan secara ilmiah, k-anonymity, l-diversity, dan differential privacy merupakan komponen esensial dari strategi perlindungan privasi konsumen digital, terutama dalam konteks database transaksi yang kaya informasi namun juga kaya risiko. Tidak ada teknik tunggal yang superior dalam semua skenario; pemilihan dan kombinasi teknik harus didasarkan pada analisis kontekstual yang mempertimbangkan jenis data, tujuan penggunaan, profil ancaman, dan persyaratan regulatif.

Kedua, terdapat tegangan yang inheren namun dapat dikelola antara kekuatan proteksi privasi dan utilitas data analitis. Pendekatan hibrid yang mengombinasikan teknik berbasis tabulasi untuk data yang dibagikan secara eksternal dengan differential privacy untuk kueri analitik, menawarkan jalur pragmatis menuju keseimbangan yang memadai. Ketiga, kerangka regulatif seperti GDPR dan UU PDP Indonesia bukan sekadar kendala kepatuhan, melainkan katalis yang mendorong organisasi untuk mengadopsi praktik pengelolaan data yang lebih bertanggung jawab dan berkelanjutan.

Berdasarkan temuan-temuan tersebut, beberapa rekomendasi dapat dikemukakan. Bagi organisasi yang mengelola database transaksi, disarankan untuk segera melakukan pemetaan data (data mapping) yang komprehensif sebagai dasar strategi anonimisasi yang berbasis risiko, dan mulai berinvestasi dalam kapasitas SDM di bidang privasi komputasional. Bagi regulator dan pembuat kebijakan, penyusunan panduan teknis yang lebih spesifik tentang standar anonimisasi dalam sektor digital merujuk pada praktik terbaik internasional namun disesuaikan dengan konteks Indonesia akan sangat membantu industri. Bagi peneliti, pengembangan teknik anonimisasi yang lebih efisien secara komputasional dan lebih adaptif terhadap karakteristik data streaming real-time merupakan frontier penelitian yang menjanjikan.

Artikel ini memiliki keterbatasan dalam hal bahwa sintesis yang dilakukan bersifat naratif dan tidak melibatkan analisis data empiris primer. Penelitian lanjutan dengan desain eksperimental misalnya, mengimplementasikan dan membandingkan teknik anonimisasi pada dataset transaksi nyata dengan metrik evaluasi yang terstandarisasi akan sangat memperkaya pemahaman tentang efektivitas praktis berbagai pendekatan yang dibahas dalam artikel ini.

DAFTAR PUSTAKA

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.

Cao, Y., & Yoshikawa, M. (2020). Quantifying differential privacy in continuous data release under temporal correlations. *IEEE Transactions on Knowledge and Data Engineering*, 33(11), 3555–3568.

Desfontaines, D., & Pejó, B. (2020). SoK: Differential privacies. *Proceedings on Privacy Enhancing Technologies*, 2020(2), 288–313.

Domingo-Ferrer, J., Sánchez, D., & Soria-Comas, J. (2021). Database anonymization: Privacy models, data utility, and microaggregation-based inter-model connections. *Synthesis Lectures on Information Security, Privacy, and Trust*, 8(1), 1–136.

European Data Protection Board. (2022). *Guidelines 01/2022 on data subject rights – Right of access*. EDPB.

Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2020). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, 42(4), 1–53.

Graef, I., Verschakelen, J., & Valcke, P. (2021). Putting the right to data portability into a competition law perspective. *Law: The Journal of the Higher School of Economics Annual Review*, 2021, 53–78.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corporation.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Sekretariat Negara RI.

Mivule, K. (2021). Utilizing noise addition for data privacy, an overview. *International Journal of Computer Science and Information Technology*, 4(2), 65–80.

Noor, N. M., Ismail, Z., & Che Harun, F. K. (2022). Adoption of data privacy practices in Southeast Asian fintech firms: Regulatory compliance and technical implementation. *Journal of Financial Crime*, 29(4), 1234–1250.

Sánchez, D., Domingo-Ferrer, J., & Martínez, S. (2021). Individual privacy in social media databases through microaggregation and data swapping. *Information Sciences*, 580, 618–635.

Tang, J., Korolova, A., Bai, X., Wang, X., & Wang, X. (2022). Privacy loss in Apple's implementation of differential privacy on MacOS 10.12. *arXiv preprint*, arXiv:1709.02753.

Voigt, P., & Von dem Bussche, A. (2021). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2nd ed.). Springer International Publishing.