KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa
Vol.4, No.1 Februari 2026

e-ISSN: 3025-5465; p-ISSN: 3025-7964, Hal 709-717

DOI: https://doi.org/10.61722/jipm.v4i1.1967

Politik Hukum Pengawasan Data Pribadi dalam Pemilu: Analisis Kasus Pencatatan NIK/KTP di SIPOL dan Tantangan Implementasi UU PDP untuk Integritas Demokrasi

Grace Febrina Simanjuntak
Universitas Prima Indonesia
Nebraska Audi Tobing
Universitas Prima Indonesia
Naomi Clara Tamba
Universitas Prima Indonesia
Jandi Rindu Saragih
Universitas Prima Indonesia

Alamat: Jalan Sampul No. 3, Medan, Sumatera Utara, Indonesia

Korespondensi penulis: febbysimanjuntak17@gmail.com, audinebraska@gmail.com, naomi.clt06@gmail.com, jandisaragih2003@gmail.com

Abstract. *The management of personal data in electoral processes has become a critical concern as it directly impacts the legitimacy of democratic governance. The emergence of cases where NIK/KTP (National Identification Numbers/Identity Cards) were recorded without the owners' consent in the Political Party Information System (SIPOL) highlights weaknesses in data protection within the electoral environment. This study examines Indonesia's legal politics in regulating and supervising the use of personal data in elections, while evaluating the extent to which the Personal Data Protection Law (UU PDP) can be applied in such cases. Using a qualitative approach based on case studies and regulatory analysis, the research finds that unclear supervision mechanisms, limited institutional capacity, and low public literacy regarding data security are major obstacles in implementing the UU PDP. These conditions pose risks to electoral integrity and may undermine public trust. The study emphasizes the need to strengthen regulatory governance, improve supervisory systems, and enhance public awareness to ensure effective personal data protection in the electoral process.*

Keywords: Personal data protection; elections; civil service; legal politics.

Abstrak. Pengelolaan data pribadi dalam proses pemilihan umum menjadi perhatian penting karena berkaitan langsung dengan legitimasi penyelenggaraan demokrasi. Terungkapnya praktik pencantuman NIK/KTP tanpa persetujuan pemilik dalam Sistem Informasi Partai Politik (SIPOL) menunjukkan masih lemahnya perlindungan data di lingkungan pemilu. Penelitian ini menelaah arah politik hukum Indonesia dalam mengatur dan mengawasi penggunaan data pribadi pada pemilu, sekaligus menilai sejauh mana Undang-undang Perlindungan Data Pribadi (UU PDP) mampu diterapkan dalam kasus tersebut. Melalui pendekatan kualitatif berbasis studi kasus dan analisis regulasi, ditemukan bahwa ketidakjelasan mekanisme pengawasan, keterbatasan kapasitas institusional, serta minimnya literasi masyarakat mengenai keamanan data menjadi

Received, Desember , 2025; Revised Desember , 2025; Februari , 2026
* Grace Febrina Simanjuntak, febbysimanjuntak17@gmail.com

hambatan utama dalam penerapan UU PDP. Kondisi tersebut menimbulkan risiko bagi integritas pemilu dan berpotensi menurunkan kepercayaan publik. Penelitian ini menekankan perlunya penguatan tata kelola regulasi, pembenahan sistem pengawasan, serta peningkatan edukasi kepada masyarakat agar perlindungan data pribadi dalam pemilu dapat berjalan efektif.

Kata kunci: Perlindungan data pribadi; Pemilu; SIPOL; Politik hukum.

PENDAHULUAN

Pemilu sebagai instrumen utama demokrasi modern menuntut adanya jaminan terhadap integritas proses dan perlindungan hak-hak warga negara, termasuk hak atas data pribadi. Dalam konteks Indonesia, isu pengawasan data pribadi dalam pemilu kembali mencuat setelah ditemukannya sejumlah kasus pencatutan Nomor Induk Kependudukan (NIK)/KTP warga ke dalam Sistem Informasi Partai Politik (SIPOL) Komisi Pemilihan Umum (KPU). Kasus ini menunjukkan bahwa penyelenggaraan pemilu tidak hanya menghadapi tantangan teknis dan administratif, tetapi juga persoalan fundamental terkait keamanan, pengelolaan, dan akuntabilitas data pribadi pemilih.

Dibentuknya Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menandai upaya negara memperkuat kerangka hukum perlindungan data di Indonesia. Namun, implementasinya dalam konteks pemilu masih menghadapi berbagai kendala, mulai dari kelembagaan, kepatuhan penyelenggara pemilu, hingga rendahnya literasi digital dan data pribadi di masyarakat. Kasus pencatutan identitas di SIPOL mengindikasikan adanya celah dalam mekanisme pendaftaran partai politik dan lemahnya kontrol internal terhadap penggunaan data pribadi.

Karena data pribadi merupakan bagian dari hak konstitusional dan menyangkut legitimasi proses demokrasi, setiap penyalahgunaan data dalam pemilu berpotensi merusak kepercayaan publik terhadap institusi politik. Oleh sebab itu, analisis politik hukum terhadap pengawasan data pribadi dalam pemilu menjadi semakin relevan, terutama dalam menilai sejauh mana UU PDP dapat diimplementasikan secara efektif untuk mencegah penyalahgunaan data dan menjaga integritas demokrasi.

Melalui pembahasan terhadap kasus pencatutan NIK/KTP di SIPOL, tulisan ini berupaya menelaah bagaimana kerangka hukum yang ada bekerja, apa saja tantangan penerapannya, serta rekomendasi arah kebijakan agar perlindungan data pribadi dapat menjadi fondasi penting dalam proses pemilu yang bersih, transparan, dan terpercaya (Republik Indonesia, 2017).

KAJIAN TEORITIS

1. Teori Politik Hukum

Politik hukum merupakan arah kebijakan dasar yang ditetapkan oleh negara dalam membentuk, menerapkan, dan menegakkan hukum guna mencapai tujuan bernegara. Menurut Mahfud MD, politik hukum dapat dipahami sebagai legal policy yang menentukan hukum mana yang akan diberlakukan atau diubah untuk menjawab kebutuhan sosial dan politik masyarakat. Dalam konteks ini, hukum tidak berdiri netral, melainkan dipengaruhi oleh konfigurasi kekuasaan, kepentingan politik, serta visi negara terhadap perlindungan hak warga negara.

Dalam penyelenggaraan pemilu, politik hukum berperan penting karena pemilu merupakan arena strategis demokrasi yang melibatkan relasi antara negara, partai politik, dan warga negara. Kebijakan hukum terkait pemilu, termasuk pengelolaan data pribadi pemilih dan anggota partai, mencerminkan sejauh mana negara menempatkan perlindungan hak konstitusional warga sebagai prioritas dibanding kepentingan administratif dan politik praktis. Oleh karena itu, pengaturan dan pengawasan penggunaan data pribadi dalam pemilu tidak dapat dilepaskan dari arah politik hukum negara dalam membangun demokrasi yang berintegritas dan berbasis perlindungan hak asasi manusia.

Penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam konteks pemilu menjadi indikator penting untuk menilai konsistensi politik hukum Indonesia. Apabila norma perlindungan data tidak diimplementasikan secara efektif dalam sistem pemilu, maka dapat disimpulkan adanya ketidaksinkronan antara kehendak normatif pembentuk undang-undang dan praktik penyelenggaraan demokrasi.

2. Teori Perlindungan Data Pribadi sebagai Hak Asasi Manusia

Perlindungan data pribadi secara teoritis berakar pada konsep hak atas privasi (right to privacy), yang diakui sebagai bagian dari hak asasi manusia. Hak privasi memberikan jaminan kepada individu untuk mengendalikan informasi pribadi yang berkaitan dengan identitas, kehidupan, dan aktivitasnya. Dalam perkembangan hukum modern, data pribadi dipandang sebagai ekstensi dari kepribadian seseorang sehingga penyalahgunaannya dapat berdampak langsung pada martabat dan kebebasan individu.

Teori perlindungan data pribadi menekankan beberapa prinsip utama, antara lain: keabsahan pemrosesan data (lawfulness), persetujuan subjek data (consent), pembatasan tujuan (purpose limitation), minimalisasi data (data minimization), keamanan data, serta akuntabilitas pengendali data. Prinsip-prinsip ini bertujuan untuk memastikan bahwa setiap pemrosesan data dilakukan secara sah, transparan, dan bertanggung jawab.

Dalam konteks pemilu, data pribadi seperti NIK/KTP memiliki sifat yang sangat sensitif karena berkaitan dengan hak politik warga negara. Penyalahgunaan data tersebut tidak hanya melanggar hak privasi, tetapi juga berpotensi memengaruhi kebebasan memilih dan keadilan kompetisi politik. Oleh karena itu, teori perlindungan data pribadi menempatkan negara dan penyelenggara pemilu sebagai pihak yang memiliki kewajiban positif untuk menjamin keamanan, keabsahan, dan penggunaan data secara proporsional.

3. Teori Tata Kelola Pemilu dan Integritas Demokrasi

Integritas pemilu merupakan konsep normatif yang merujuk pada penyelenggaraan pemilu yang bebas, adil, transparan, dan dapat dipercaya oleh publik. Menurut teori tata kelola pemilu (electoral governance), integritas pemilu tidak hanya ditentukan oleh prosedur pemungutan suara, tetapi juga oleh keseluruhan siklus pemilu, termasuk pengelolaan data pemilih, pendaftaran partai politik, serta sistem informasi pemilu.

Dalam era digital, sistem informasi pemilu menjadi elemen krusial yang memengaruhi legitimasi hasil pemilu. Ketika pengelolaan data pribadi dalam sistem tersebut tidak aman atau tidak akuntabel, maka integritas pemilu turut terancam. Teori ini menegaskan bahwa kepercayaan publik terhadap pemilu sangat bergantung pada kemampuan penyelenggara pemilu dalam melindungi data, mencegah manipulasi, serta menyediakan mekanisme pengawasan yang efektif.

Lemahnya pengawasan data pribadi dapat menimbulkan persepsi ketidakadilan, membuka peluang penyalahgunaan politik berbasis data, dan pada akhirnya menurunkan legitimasi demokrasi. Dengan demikian, perlindungan data pribadi bukan sekadar isu teknis, melainkan bagian integral dari upaya menjaga kualitas dan integritas demokrasi.

4. Kerangka Teoretis Analisis

Berdasarkan teori politik hukum, teori perlindungan data pribadi, dan teori integritas pemilu, penelitian ini memposisikan pengawasan data pribadi dalam pemilu sebagai pertemuan antara kebijakan hukum negara, perlindungan hak asasi warga negara, dan kualitas demokrasi. Kasus pencatutan NIK/KTP dalam SIPOL dianalisis sebagai cerminan dari lemahnya implementasi politik hukum perlindungan data pribadi dalam arena pemilu.

Kerangka teoretis ini digunakan untuk menilai sejauh mana UU PDP mampu berfungsi sebagai instrumen perlindungan hak dan penjaga integritas pemilu, sekaligus mengidentifikasi faktor struktural, kelembagaan, dan sosial yang menghambat efektivitas pengawasannya. Dengan demikian, kajian teoritis ini menjadi dasar konseptual dalam menganalisis temuan penelitian dan merumuskan rekomendasi kebijakan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis-normatif yang dipadukan dengan pendekatan socio-legal untuk menelaah politik hukum pengawasan data pribadi dalam penyelenggaraan Pemilu, khususnya terkait kasus pencatutan NIK/KTP pada Sistem Informasi Partai Politik (SIPOL). Pendekatan yuridis-normatif digunakan untuk menganalisis norma-norma hukum positif yang mengatur perlindungan data pribadi, mekanisme verifikasi pemilih dan anggota partai, serta kewajiban penyelenggara Pemilu sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-undang Pemilu, dan peraturan teknis Komisi Pemilihan Umum (KPU). Analisis dilakukan melalui interpretasi gramatikal, sistematis, dan teleologis guna mengidentifikasi ruang lingkup kewenangan, kewajiban, serta potensi celah hukum yang menyebabkan terjadinya penyalahgunaan identitas.

Pendekatan socio-legal digunakan untuk membaca praktik implementasi hukum di lapangan, termasuk pola pengawasan KPU, efektivitas mekanisme perlindungan data, serta dampak pencatutan data terhadap kepercayaan publik dan integritas demokrasi. Data empiris diperoleh melalui studi dokumen, laporan pengaduan publik, putusan atau rekomendasi lembaga pengawas (jika relevan), serta pemberitaan yang telah terverifikasi. Teknik analisis kualitatif digunakan untuk menafsirkan temuan empiris dan menghubungkannya dengan kerangka normatif, sehingga dapat disimpulkan bagaimana konfigurasi politik hukum memengaruhi efektivitas perlindungan data pribadi dalam tahapan Pemilu.

HASIL PENELITIAN DAN PEMBAHASAN

A. Bentuk Kerentanan Perlindungan Data Pribadi dalam Kasus Pencatutan NIK/KTP dalam SIPOL

Dalam konteks regulasi nasional mengenai perlindungan data pribadi, kasus pencatutan NIK/KTP dalam Sistem Informasi Partai Politik (SIPOL) menunjukkan keterputusan antara norma hukum dan implementasi teknis di lapangan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara tegas menempatkan pengendalian data pada prinsip dasar seperti keabsahan pemrosesan (*lawful processing*), pembatasan tujuan, minimalisasi data, dan kewajiban memperoleh persetujuan eksplisit (*explicit consent*) dari pemilik data (Republik Indonesia, 2022). Penjelasan umum UU PDP bahkan menegaskan bahwa pengumpulan dan pemrosesan data harus menjamin hak privasi setiap warga negara serta memberikan kontrol penuh kepada individu terhadap penggunaan data pribadinya oleh pihak lain (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022). Namun, praktik di SIPOL justru memperlihatkan bahwa pemrosesan data dilakukan tanpa mekanisme persetujuan yang sah, karena seseorang dapat dicatat sebagai anggota partai politik tanpa pernah memberikan otorisasi. Hal ini menunjukkan bahwa sistem digital penyelenggara pemilu belum menjalankan prinsip-prinsip dasar perlindungan data sebagaimana dirumuskan dalam regulasi.

Selain itu, UU PDP mengamanatkan adanya tanggung jawab pengendali data (*data controller*) untuk memastikan penerapan aspek keamanan, termasuk mekanisme autentikasi, pembatasan akses, dan pengawasan aktivitas pemrosesan data (Republik Indonesia, 2022). Namun, SIPOL masih menunjukkan kelemahan struktural dalam pengelolaan akses internal, di mana operator partai dapat mengunggah data identitas tanpa proses verifikasi langsung dari pemilik data. Padahal, regulasi menekankan bahwa pengendali data wajib menerapkan kebijakan teknis dan operasional yang berbasis pada resiko (*risk-based approach*) untuk mencegah penyalahgunaan. Dalam konteks ini, ketidakmampuan SIPOL untuk mendeteksi dan mencegah pencatutan identitas—termasuk tidak adanya sistem deteksi anomali, audit trail yang memadai, dan pemberitahuan kepada subjek data—menunjukkan bahwa standar keamanan dan akuntabilitas belum terpenuhi. Lebih jauh, UU PDP memberikan hak bagi subjek data untuk menghapus data yang tidak akurat atau tidak sah, namun mekanisme pemulihan data dalam SIPOL masih sangat terbatas sehingga hak tersebut tidak dapat dijalankan secara efektif. Dengan demikian, praktik pemrosesan data dalam SIPOL secara nyata bertentangan dengan konsep perlindungan data pribadi yang menempatkan hak subjek data sebagai pusat pengaturan, sehingga menuntut pembenahan teknis dan kelembagaan untuk memastikan kesesuaian dengan rezim regulasi nasional.

B. Upaya kebijakan apa yang diperlukan untuk memperkuat mekanisme pengawasan data pribadi dalam pemilu guna memastikan integritas demokrasi

Pengawasan data pribadi dalam pemilu merupakan aspek krusial untuk menjaga kepercayaan publik, mencegah manipulasi politik berbasis data, serta memastikan bahwa proses demokrasi berlangsung secara adil. Dalam konteks digitalisasi data pemilih, peningkatan keamanan dan regulasi menjadi keharusan agar data tidak disalahgunakan untuk kepentingan tertentu.

Beberapa kebijakan yang diperlukan untuk memperkuat mekanisme pengawasan data pribadi dalam pemilu antara lain:

1. Penerapan regulasi perlindungan data pribadi yang tegas dan terukur

Undang-undang serta aturan teknis harus memberikan batasan jelas mengenai bagaimana data pemilih dikumpulkan, disimpan, diproses, dan dibagikan. Termasuk di dalamnya penetapan standar enkripsi, kewajiban persetujuan pengguna (*consent*), serta sanksi tegas terhadap kebocoran data dan penyalahgunaan oleh pihak ketiga.

2. Pembentukan lembaga pengawas independen khusus data pemilu

Lembaga ini memiliki fungsi audit, investigasi, dan penegakan hukum terkait pelanggaran data pribadi selama pemilu. Independen dari partai politik atau lembaga penyelenggara, guna menghindari konflik kepentingan.

3. Audit keamanan digital secara berkala

Sistem informasi pemilih harus menjalani pemeriksaan keamanan secara rutin untuk mendeteksi celah kerentanan. Audit dilakukan oleh tim profesional keamanan siber yang bersertifikasi dan dilaporkan secara transparan kepada publik.

4. Transparansi pengelolaan data bagi masyarakat

Publik berhak mengetahui data apa saja yang dikumpulkan, untuk keperluan apa, serta bagaimana penyimpanannya. Transparansi dapat meningkatkan pengawasan partisipatif masyarakat terhadap penyelenggara pemilu.

5. Peningkatan literasi digital dan kesadaran keamanan data

Pemilih perlu dibekali pemahaman mengenai risiko penyebaran data pribadi, potensi penipuan digital, serta bagaimana melindungi data mereka dari penyalahgunaan. Kampanye literasi data harus menjadi bagian dari agenda pemilu nasional.

6. Pengaturan teknologi AI dan Big Data dalam kampanye politik

Untuk mencegah micro-targeting politik yang dapat memanipulasi preferensi pemilih berdasarkan data pribadi, negara harus menetapkan batasan pemanfaatan big data dan algoritma kampanye berbasis profiling.

7. Kerja sama internasional dalam standar perlindungan data pemilu

Mengadaptasi standar global seperti GDPR serta bertukar praktik terbaik dengan negara lain dapat memperkuat kualitas pengamanan data nasional.

Dengan penerapan kebijakan tersebut, sistem pengawasan data pribadi dalam pemilu dapat menjadi lebih kokoh, mengurangi potensi kebocoran dan penyalahgunaan, serta menjaga integritas pemilu sebagai fondasi demokrasi.

C. Dampak Lemahnya Pengawasan Data Pribadi terhadap Integritas Pemilu dan Kepercayaan Publik.

Di zaman digital yang terus berkembang saat ini, proses pemilihan umum sering melibatkan pengumpulan dan analisis data dalam jumlah besar, termasuk informasi pribadi dari pemilih. Situasi ini menimbulkan ancaman dalam bidang keamanan siber, seperti peretasan dan penyebaran informasi tidak benar, yang berpotensi memengaruhi hasil pemilihan (Morozov, 2013). Namun, analisis menunjukkan bahwa angka serangan siber di seluruh dunia mengalami peningkatan setiap tahunnya. Ketika kita meneliti lebih lanjut, tipe serangan yang paling meluas adalah malware dan kelemahan sistem. Serangan siber yang memanfaatkan malware menjadi salah satu jenis ancaman keamanan digital yang paling sering terjadi dan paling berbahaya. Malware merupakan singkatan dari perangkat lunak berbahaya, yaitu istilah yang menggambarkan berbagai jenis perangkat lunak yang dirancang untuk merusak, mengganggu, atau memberikan akses ilegal ke sistem komputer. Di sisi lain, serangan siber yang memanfaatkan kerentanan berkaitan dengan eksploitasi celah atau kelemahan yang terdapat dalam sistem keamanan, perangkat lunak, atau perangkat keras (National Cyber Security Center, 2016). Penyerang memanfaatkan kelemahan ini untuk mengakses secara ilegal, mencuri informasi, atau menyebabkan kerusakan. Bentuk serangan siber, baik melalui malware maupun kerentanan, dapat mengancam berbagai sektor, termasuk dalam konteks pemilihan umum. Hal yang paling penting dalam isu ini adalah melindungi data para pemilih.

Lemahnya pengawasan terhadap data pribadi pemilih menimbulkan ancaman serius bagi integritas pemilu dan stabilisasi demokrasi. Ketika data pemilih mudah bocor atau disalahgunakan, muncul potensi manipulasi seperti penggandaan suara, penyusunan daftar pemilih yang tidak akurat, atau penggunaan data untuk kampanye politik yang tidak etis. Situasi ini mengurangi transparansi dan merusak keadilan proses pemilu (Pradnyana & Sasmita, 2024)

Dampak lainnya adalah menurunnya kepercayaan masyarakat. Kebocoran data membuat pemilih merasa tidak aman dan meragukan kemampuan negara melindungi informasi mereka. Ketika masyarakat menilai proses pemilu tidak profesional dan rentan penyalahgunaan, legitimasi

hasil pemilu ikut dipertanyakan (Kusuma & Yanto, 2024) Hal ini berpotensi menurunkan tingkat partisipasi pemilih serta melemahkan kepercayaan publik terhadap institusi demokrasi.

Selain itu, lemahnya perlindungan data memperbesar celah bagi serangan siber yang dapat mengganggu sistem pendaftaran pemilih maupun penghitungan suara (Hilmi & Hernawati, 2024) Kerentanan ini menunjukkan bahwa demokrasi modern tidak hanya bergantung pada aturan pemilu, tetapi juga pada keamanan digital yang kuat (Pradnyana et al., 2024; Hilmi et al., 2024).

Dampak dari bocornya data peserta pemilu ini tidak bisa dianggap sebagai suatu masalah yang sepele. Bocornya data ini akan memberikan dampak negatif bagi KPU RI yang merupakan lembaga yang seharusnya dipercaya oleh masyarakat akan tetapi dengan adanya permasalahan tersebut akan mempengaruhi tingkat kepercayaan masyarakat kepada KPU RI. Dengan adanya kebocoran data ini memberikan peluang kepada oknum-oknum yang tidak bertanggungjawab tersebut akan menyalahgunakan data pribadi yang bocor tersebut untuk kepentingan pribadinya.

Kebocoran data daftar pemilih tetap Pemilu di Indonesia ini merupakan suatu masalah yang krusial, mengingat bahwa kejadian peretasan data ini bukanlah peristiwa yang terjadi pertama kali di situs KPU RI. Peretasan data ini melahirkan asumsi-asumsi mengenai data pemilih yang tidak terdata atau bahkan menyasar. Dengan adanya asumsi tersebut memberikan rasa kekhawatiran kepada masyarakat yang memiliki hak untuk memilih yang mana oknum-oknum yang tidak bertanggungjawab tersebut dapat memanfaatkan hal tersebut.

KESIMPULAN

Berdasarkan hasil pembahasan mengenai politik hukum pengawasan data pribadi dalam penyelenggaraan Pemilu, dapat disimpulkan bahwa kasus pencatutan NIK/KTP dalam SIPOL menunjukkan adanya kesenjangan serius antara norma hukum dalam UU Perlindungan Data Pribadi (UU PDP) dan implementasinya di lapangan. Meskipun UU PDP telah menetapkan prinsip keabsahan pemrosesan, persetujuan eksplisit, keamanan data, serta akuntabilitas pengendali data, SIPOL belum menerapkan standar tersebut secara memadai sehingga memberikan ruang terjadinya penyalahgunaan identitas tanpa persetujuan pemilik data. Kelemahan sistem autentikasi, akses internal yang tidak terkontrol, serta minimnya mekanisme deteksi anomali mengindikasikan perlunya pembenahan mendasar dalam tata kelola sistem digital penyelenggara pemilu.

Dari sisi kebijakan, pengawasan data pribadi dalam pemilu masih terhambat oleh ketidakjelasan pembagian kewenangan antar-lembaga, lemahnya kapasitas institusional, serta kurangnya audit keamanan yang bersifat rutin dan transparan. Selain itu, rendahnya literasi digital masyarakat memperburuk kerentanan terhadap pencatutan data dan membuka peluang penyalahgunaan lebih lanjut oleh pihak tidak bertanggung jawab. Kondisi ini menunjukkan bahwa rezim perlindungan data pribadi dalam pemilu belum berfungsi secara efektif untuk menjamin keadilan dan integritas demokrasi.

Lemahnya pengawasan data pribadi membawa dampak signifikan terhadap integritas pemilu dan kepercayaan publik. Kebocoran identitas pemilih, manipulasi data, dan potensi serangan siber tidak hanya mengancam validitas daftar pemilih, tetapi juga menurunkan kredibilitas penyelenggara pemilu. Ketika pelanggaran data berulang, legitimasi hasil pemilu ikut dipertanyakan dan partisipasi pemilih dapat menurun. Oleh karena itu, diperlukan penguatan kerangka regulasi, peningkatan standar keamanan digital, pembentukan mekanisme pengawasan independen, serta edukasi publik yang berkelanjutan agar perlindungan data pribadi dapat menjadi fondasi utama dalam mewujudkan pemilu yang transparan, bebas manipulasi, dan dipercaya masyarakat.

DAFTAR PUSTAKA

Hilmi, M., Fakhriah, E., & Hernawati, E. (2024). Perlindungan data pribadi dalam pemilihan umum: Tanggung jawab hukum dan strategi penerapan. *Iustitia Omnibus.*

Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). Penjelasan umum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kominfo.

Kusuma, H., & Yanto, A. (2024). The integrity of elections: Urgency of personal data protection in modern democracy. *International Journal of Social Science and Human Research.*

Pradnyana, P. R., Utama, I. W., & Sasmita, D. K. (2024). Securing democracy in cyberspace: Voter data leaks in Indonesia's 2024 election. *Jurnal Trias Politika*.

Republik Indonesia. (2017). Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.