ANALISIS YURIDIS TANGGUNG JAWAB HUKUM NEGARA TERHADAP KEBOCORAN DATA PEMILIH TETAP PADA KOMISI PEMILIHAN UMUM

Ananda Putra Andrean[1],
Anna Triningsih[2],
Ahluddin Saiful Ahmad[3]

[1,2,3] Universitas Esa Unggul
aputraandrean@gmail.com

LPPM STIA Said Perintah Volume 4, No. 1, Maret 2023
https://stia-saidperintah.e-journal.id/ppj

Received; 2026-08-15
Accepted; 2026-08-30
Published; 2026-09-06

Abstrak

Penelitian ini membahas tanggung jawab negara dalam menjamin perlindungan data pribadi warga negara berdasarkan ketentuan peraturan perundang-undangan serta menganalisis dampak kebocoran Data Pemilih Tetap (DPT) yang dikelola oleh Komisi Pemilihan Umum (KPU) ditinjau dari perspektif hak asasi manusia. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, yang didukung oleh kajian terhadap berbagai sumber hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa negara memiliki kewajiban untuk melindungi data pribadi sebagai bagian dari pemenuhan hak atas privasi yang dijamin oleh konstitusi dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Akan tetapi, terjadinya kebocoran DPT mengindikasikan bahwa pelaksanaan perlindungan data di lingkungan lembaga publik belum berjalan secara optimal. Peristiwa tersebut tidak hanya menimbulkan risiko penyalahgunaan data pribadi, tetapi juga berpotensi mengurangi kepercayaan masyarakat terhadap penyelenggaraan pemilu dan pemerintahan. Oleh sebab itu, diperlukan penguatan tata kelola data, peningkatan kapasitas keamanan siber, serta penegakan hukum yang konsisten untuk menjamin perlindungan hak privasi warga negara di era digital.

Kata kunci: Hak Asasi Manusia; Perlindungan Data Pribadi; Tanggung Jawab Negara.

PENDAHULUAN

Transformasi digital yang cepat telah merevolusi tata kelola pemerintahan masa kini. Hampir semua layanan masyarakat, mulai dari pengelolaan data warga, urusan pajak, layanan medis, sistem pendidikan, sampai program bantuan kesejahteraan, kini beroperasi melalui sistem elektronik yang saling terhubung via wadah berbasis teknologi terpadu. Untuk menjalankan sistem tersebut lembaga pemerintahan, dipaksa mengumpulkan, mengolah, dan menyimpan data kependudukan warga dalam skala masif dan berkesinambungan, pada konteks tersebut, data pribadi tidak lagi sekadar informasi administratif, tetapi menjadi aset strategis negara yang menja-di tulang punggung penyelenggaraan layanan publik, perencanaan kebijakan, dan pengambilan keputusan berbasis data. Berlangsung pelayanan yang baik terlihat bagaimana data bisa saling berintegrasi serta mampu melindungi data yang terdapat didalamnya agar tidak terjadinya kebobolan data untuk bisa tersebar luas secara illegal untuk bisa dimanfaatkan oleh pihak yang tidak bertanggungjawab (Angraini K et al., 2024).

Namun seiring dengan peran strategis tersebut, muncul pula risiko besar dimana data pribadi warga menjadi titik rawan terhadap kebocoran, penyalahguna-an dan serangan siber jika tidak dikelola dengan standar keamanan serta pengaturan yang cukup. Insiden kebocoran data pribadi di lingkungan lembaga pemerin-tahan kini tidak bisa lagi hanya dilihat sebagai gangguan teknis, tetapi sebagai permasalahan struktural dengan berkenaan langsung dari hak privasi serta perlindung-an data pribadi warga sebagai satu diantara hak asasi manusia. Di sinilah letak kewajiban konstitusional negara: di saat yang sama mengelola data pribadi warga dalam skala besar, otoritas negara juga wajib menyusun sistem yang transparan, aman, dan akuntabel, serta memenuhi kewajiban hukum perlindungan data pribadi menurut regulasi nasional, termasuk ketentuan pada undang-undang yang mengaturnya (Anggen Suari & Sarjana, 2023).

Pada konteks tersebut ,Indonesia memiliki sejumlah insiden penyebaran data ilegal yang melibatkan data pribadi warga di lingkungan otoritas negara menunjukkan tingkat kerentanan sistem data yang tinggi. Salah satu contoh paling disorot adalah kebocoran data yang terdapat dalam Daftar Pemilih Tetap (DPT) pada Komisi Pemilihan Umum (KPU) tahun 2023. Insiden tersebut menunjukkan ketidakberhasilan pemerin-tah dalam memberikan pelindungan data pribadi Pemilih, yang menyebabkan bocornya 204 juta data kependudukan yang diambil dari *database* SIDALIH (Sistem Informasi Data Pemilih) (Tri Wibowo,2024).

Data SIDALIH tersebut, telah diduga diperjualbelikan pada forum *daring* dan memuat berbagai informasi pribadi, seperti Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga, alamat, tempat dan tanggal lahir, serta informasi administratif lainnya. Besarnya jumlah data yang bocor menunjukkan adanya ancaman terhadap sistem pengelolaan data pemilih tidak hanya berasal dari serangan eksternal, tetapi juga dapat dipengaruhi oleh kelemahan tata kelola keamanan informasi di lingkungan organisasi. Selain menimbulkan risiko penyalahgunaan identitas dan tindak kejahatan siber, insiden tersebut juga berpotensi menurunkan legitimasi institusi penyelenggara pemilu karena masyarakat menilai bahwa negara belum mampu memberikan perlindungan yang memadai terhadap data pribadi yang dipercayakan kepadanya. Kondisi ini memperlihatkan bahwa keamanan data pemilih harus dipandang sebagai bagian integral dari perlindungan hak warga negara dalam proses demokrasi (Kunto & Wibowo, 2024).

Dalam pelaksanaan tahapan pemilu, KPU memiliki kewenangan untuk melakukan pemutakhiran, pengelolaan, serta penyusunan daftar pemilih yang menjadi dasar pelaksanaan hak politik warga negara. Tanggung jawab tersebut diberikan oleh Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum dan dijabarkan lebih lanjut melalui berbagai Peraturan Komisi Pemilihan Umum Nomor 4 Tahun 2025 tentang Perubahan Kedua atas Peraturan Komisi Pemilihan Umum Nomor 22 Tahun 2023 tentang Pengelolaan dan Pelayanan Informasi Publik di Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/ Kota, yang mengatur mekanisme penyusunan serta pemeliharaan data pemilih. Posisi KPU sebagai pengelola data pemilih menempatkan lembaga ini sebagai pengendali data yang memproses informasi pribadi dalam jumlah besar, mulai dari identitas kependudukan hingga data administratif lainnya.

Oleh karena itu, pengelolaan data pemilih tidak hanya berkaitan dengan kebutuhan administratif penyelenggaraan pemilu, tetapi juga berkaitan dengan kewajiban hukum untuk menjamin keamanan, kerahasiaan, dan integritas data yang dikelola. Seiring meningkatnya digitalisasi sistem

pemilu, tuntutan terhadap perlindungan data pribadi menjadi semakin penting karena kualitas tata kelola data pemilih turut menentukan tingkat kepercayaan masyarakat terhadap proses demokrasi yang berlangsung (Alfian Kusnaldi et al., 2022)

Kasus kebocoran data nasional tahun 2024 menunjukkan bahwa otoritas negara, dalam hal ini KPU sebagai pihak yang bertanggung jawab yang berperan sebagai pengendali data publik skala besar, namun tidak sepenuhnya mampu melaksanakan kewajiban hukum perlindungan data secara efektif (Rusyda,2025). Padahal amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menuntut penerapan mekanisme pemberitahuan insiden, transparansi, dan tanggung jawab akuntabilitas kepada subjek data, padahal dalam pratiknya keterlambatan dalam pemberitahuan insiden kepada subjek data serta minimnya informasi yang dibuka kepada publik, berdampak pada pembangkangan terhadap UU PDP. Temuan tersebut menunjukkan lemahnya sistem keamanan siber, rendahnya transparansi informasi kepada publik, serta respons yang dinilai lambat setelah kebocoran terjadi.

Di sisi lain, analisa hukum terhadap penyebaran data pribadi secara umum menegaskan bahwa pasal-pasal tanggung jawab pengendalian data dalam peraturan tersebut memberikan landasan hukum baik bagi pengenaan sanksi administratif maupun pidana, serta hak pemilik data pribadi dalam menggugat dan memperoleh ganti kerugian jika terjadi penyalahgunaan. Namun, dalam praktik lingkungan otoritas negara, kewajiban dan sanksi tersebut masih sering tidak diimplementasikan secara konsisten, sehingga risiko kebocoran data pribadi tetap tinggi (Andi Prasetyo and Ariadi, 2025).

Dalam sistem ketatanegaraan Indonesia, perlindungan hak asasi manusia merupakan salah satu prinsip fundamental yang menjadi dasar penyelenggaraan negara hukum. Jaminan tersebut ditegaskan dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945), yang menempatkan hak-hak warga negara secara lebih komprehensif dalam Bab II. Pengaturan tersebut menunjukkan bahwa negara memiliki kewajiban untuk menghormati, melindungi, dan memenuhi hak-hak dasar setiap individu tanpa terkecuali. Selain memperoleh pengakuan secara konstitusional, perlindungan HAM juga diperkuat melalui Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) yang menegaskan tanggung jawab negara dalam menjamin terlaksananya hak-hak warga negara. Dalam perkembangannya, konsep perlindungan HAM tidak lagi terbatas pada hak-hak sipil dan politik, tetapi juga mencakup berbagai hak yang muncul sebagai konsekuensi perkembangan teknologi dan digitalisasi kehidupan masyarakat. Oleh karena itu, setiap kebijakan maupun tindakan pemerintah, termasuk dalam pengelolaan informasi dan data pribadi warga negara, harus dilaksanakan dengan tetap berpedoman pada prinsip-prinsip perlindungan HAM yang telah dijamin oleh konstitusi dan peraturan perundang-undangan (Hakim & Kurniawan, 2021).

Hak atas privasi saat ini diakui sebagai bagian dari hak asasi manusia yang harus dilindungi oleh negara. Dalam perspektif HAM, privasi tidak hanya berkaitan dengan kehidupan pribadi seseorang, tetapi juga mencakup perlindungan terhadap data dan informasi yang melekat pada identitas individu. Pengakuan tersebut tercermin dalam berbagai instrumen HAM internasional serta Pasal 28G ayat (1) UUD NRI Tahun 1945 yang menjamin perlindungan diri pribadi dan rasa aman setiap warga negara. Dalam era digital, data pribadi menjadi bagian penting dari hak privasi sehingga setiap kebocoran atau penyalahgunaan data berpotensi menimbulkan pelanggaran HAM. Oleh karena itu, negara memiliki kewajiban untuk menjamin keamanan data pribadi warga sebagai bentuk perlindungan terhadap hak privasi (Argiansyah et al., 2024).

Rangkaian kasus terserbut menunjukan lemahnya keamanan data serta akuntabilitas otoritas negara dan Fenomena ini menegaskan bahwa kebocoran data pribadi oleh otoritas negara bukan kejadian tunggal, melainkan pola yang berulang jika tidak disertai dengan perbaikan regulasi, penegakan hukum, dan tata kelola internal yang lebih ketat.

Beberapa kajian literatur terstruktur terhadap kebocoran data pribadi di Indonesia menemukan bahwa penyebab utama insiden berasal dari kelemahan SOP, kemampuan tenaga kerja, dan tata kelola perlindungan dunia maya yang belum kuat di lingkungan instansi pemerintah. Di sisi lain, penelitian tentang pola kebocoran data pribadi secara umum menunjukkan bahwa insiden cenderung meningkat karena lemahnya sistem keamanan informasi, minimnya regulasi yang komprehensif, serta rendahnya kesadaran publik mengenai risiko pemanfaatan data pribadi oleh otoritas negara (Seta Ari Yuwana et al, 2025). Dalam konteks itu, otoritas negara sekaligus berperan sebagai penggalang kepercayaan publik atas kebijakan digital sekaligus menjadi penyebab ketidakpercayaan jika tidak mampu

mengelola data pribadi dengan standar keamanan yang memadai.

Dari perspektif HAM, dampak kebocoran DPT insiden tersebut menimbulkan pelanggaran hak privasi serta proteksi data pribadi warga negara. Kebocoran data pribadi yang melibatkan nomor identitas nasional, alamat, riwayat administratif, dan data layanan publik membuka potensi penyalahgunaan, diskriminasi, dan pelanggaran kebebasan pribadi. Dalam kerangka konstitusional, hak atas privasi tercakup dalam HAM yang dilindungi oleh negara, sehingga kebocoran basis data individu oleh otoritas negara dapat dipandang sebagai pelanggaran hak konstitusional jika tidak diikuti mekanisme pemulihan dan perlindungan yang memadai.

Di tingkat kebijakan, insiden kebocoran data di lingkungan otoritas negara menimbulkan beberapa persoalan krusial di antaranya lemahnya sistem keamanan siber dan tata kelola data di sektor publik, keterbatasan peraturan pelaksana dan lembaga pengawas yang independen, serta menurunnya keper-cayaan publik terhadap pemerintah untuk mengelola dan melindungi data pribadi warga. Sejumlah kajian kebijakan pemerintah menegaskan perlunya penguatan regulasi, peningkatan kapasitas teknis, dan pembentukan otoritas pengawas data yang independen untuk memastikan bahwa otoritas negara tidak menjadi sumber utama risiko kebocoran data (Utami et al, 2025). Di sisi lain, penelitian tentang kebocoran data pribadi di Indonesia menunjukkan bahwa upaya pencegahan selama ini masih terfokus pada aspek teknis, tanpa integrasi kuat dengan dimensi hukum, hak subjek data, dan transparansi pemerintahan.

Dalam kerangka penelitian, penting untuk memetakan bagaimana otoritas negara berperan sebagai pengendali informasi individu sekaligus berkontribusi terhadap terjadinya penyebaran data secara ilegal, serta sejauh mana ketentuan hukum sebagaimana UU PDP mampu mengurangi risiko kebocoran tersebut di lingkungan sektor publik. Sejumlah kajian terbaru telah menyoroti aspek teknis, regulasi, dan tata kelola data pribadi oleh otoritas negara, namun mayoritas masih berfokus pada analisis kasus teknis atau sektor tertentu, tanpa mengintegrasikan analisis konstitusional, hak privasi, dan dampak politik-sosial secara utuh. Kekosongan penelitian ini menciptakan celah besar, terutama di kajian normatif yang mengkaji hubungan antara tanggung jawab hukum negara, perlindungan hak privasi warga, dan kewajiban pengendalian data pribadi oleh otoritas negara.

Urgensi penelitian ini semakin tinggi jika dikaitkan dengan meningkatnya insiden kebocoran data di lingkungan otoritas negara, seperti insiden pelanggaran kebocoran data pribadi oleh otoritas negara tidak hanya mengganggu layanan publik dan menimbulkan kerugian ekonomi, tetapi juga mengancam hak privasi sebagai hak asasi manusia dan merusak kepercayaan publik terhadap pemerintah. Berangkat dari gap dan urgensi tersebut, arah penelitian ini menekankan pada analisis kerangka hukum UU PDP, pemenuhan kewajiban perlindungan data pribadi oleh otoritas negara, serta kelemahan normatif-regulatif yang membuat negara tetap menjadi sumber risiko kebocoran data, sehingga rumusan masalah nantinya menyoroti pertanggungjawaban hukum negara, perlindungan hak privasi, dan efektivitas regulasi terhadap pemerintah.

Berdasarkan uraian latar belakang tersebut diatas, penelitian ini merumuskan permasalahan sebagai berikut:

1. Bagaimana pengaturan tanggung jawab Negara dalam melindungi data pribadi warga Negaranya berdasarkan Peraturan Perundang-Undangan?
2. Bagaimana implikasi tanggung jawab Negara terhadap kebocoran Data Pemilih Tetap di Komisi Pemilihan Umum dalam perspektif Hak Asasi Manusia?

Untuk menjawab permasalahan tersebut, penelitian ini menggunakan jenis penelitian hukum normatif, yang menggambarkan suatu rangkaian pola pikir serta tindakan manusia yang berlandaskan pada norma-norma umum yang berlaku di masyarakat, tanpa membedakan status sosial ataupun peran individu dalam lingkup sosialnya (Amiruddin, 2016). Dalam penelitian, penulis menelusuri dan mengumpulkan acuan hukum yang sesuai di Indonesia, terutama yang berfokus pada topik tema penelitian mengenai tanggung jawab hukum negara dalam melindungi data pribadi warga negara.

METODE PENELITIAN

Adapun pendekatan penelitiannya menggunakan pendekatan perundang-undangan (*statute approach*) serta pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan hukum yang berkaitan dengan objek penelitian. Disisi

lain pendekatan konseptual dipakai guna mengkaji berbagai hal yang berkaitan langsung dengan norma-norma hukum yang tercantum pada berbagai regulasi di Indonesia serta digunakan teori dan asas hukum yang mendasari analisis terhadap responsibilitas hukum Negara guna melindungi data pribadi warga negara serta kelemahan Implementasi UU PDP terhadap kasus kebocoran data di Indonesia, sehingga riset yang berlangsung sekarang mampu mengasihi pemahaman hukum yang jelas dan menyeluruh (Jonaedi, 2024).

Sedangkan sumber penelitian menggunakan sumber data sekunder yang mencakup berbagai jenis bahan hukum yaitu bahan hukum primer, bahan hukum sekunder serta bahan hukum tersier. Adapun penjabaran dari tiap jenis bahan hukum tersebut yakni seperti:

1. Bahan Hukum Primer, dengan berlandaskan atas bahan riset dengan bermuara oleh bahan hukum yang menyatu yang berkesesuaian dari judul rumusan masalah riset yakni:
    A. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
    B. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah terakhir dengan Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
    C. Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
    D. Undang Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia;
    E. Undang Undang Nomor 7 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2022 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum menjadi Undang-Undang
    F. Peraturan Komisi Pemilihan Umum Nomor 4 Tahun 2025 tentang Perubahan Kedua atas Peraturan Komisi Pemilihan Umum Nomor 22 Tahun 2023 tentang Pengelolaan dan Pelayanan Informasi Publik di Komisi Pemilihan Umum, Komisi Pemilihan Umum Provinsi, dan Komisi Pemilihan Umum Kabupaten/Kota.

2. Bahan Hukum Sekunder, berfungsi sebagai pelengkap dan penguat materi primer, sekaligus berbagai sumber literatur yang membantu memberikan penjelasan dan pemahaman pada tahapan berikutnya mengenaik bahan hukum primer. Berbagai referensi sumber bahan hukum untuk penelitian ini terdiri dari buku-buku dan jurnal ilmiah terkait, artikel, hasil-hasil penelitian sebelumnya, serta karya akademik lainnya untuk membantu peneliti memperluas sudut pandang, memperkuat dasar teori, dan memperdalam analisis terhadap masalah hukum yang menjadi pokok kajian.
3. Bahan Hukum Tersier, diartikan layaknya materi referensial dengan mengakomodir penguraian komprehensif serta pedoman praktis oleh instrumen hukum primer serta sekunder. Manifestasinya mampu ditemui pada leksikon (KBBI), ensiklopedia.

Untuk teknik pengumpulan bahan hukum memakai penelitian kepustakaan yang dilakukan secara terstruktur terhadap berbagai dokumen serta literatur hukum yang relevan. Setelah seluruh bahan hukum terkumpul, tahap berikutnya adalah pengolahan data melalui proses seleksi dan kategorisasi berdasarkan rumusan masalah yang diteliti.

Sedangkan teknik analisis bahan hukum yang dipakai yakni metode analisis kualitatif dengan pendekatan preskriptif, yakni analisis yang bertujuan menilai apakah suatu praktik atau kebijakan selaras dengan ketentuan hukum yang berlaku, serta mengkaji apa yang seharusnya dilakukan menurut hukum dalam konteks potensi konflik kepentingan hakim.

ANALISIS DAN PEMBAHASAN

A. Pengaturan Tanggung Jawab Negara Dalam Melindungi Data Pribadi Warga Negaranya Berdasarkan Peraturan Perundang-Undangan

Perkembangan teknologi informasi yang semakin pesat telah mendorong meningkatnya aktivitas pengumpulan, penyimpanan, dan pemanfaatan data pribadi dalam berbagai sektor kehidupan. Kondisi tersebut menimbulkan kebutuhan akan perlindungan hukum yang memadai guna menjamin keamanan data pribadi masyarakat. Dalam konteks negara hukum, perlindungan data pribadi merupakan bagian dari upaya negara untuk menjamin hak asasi manusia, khususnya hak atas privasi.

Di Indonesia, jaminan tersebut berlandaskan Pasal 28G ayat (1) UUD NRI Tahun 1945 yang memberikan perlindungan terhadap diri pribadi, kehormatan, martabat, serta rasa aman setiap warga negara. Oleh karena itu, negara memiliki kewajiban konstitusional untuk memastikan bahwa data pribadi masyarakat terlindungi dari berbagai bentuk penyalahgunaan maupun akses yang tidak sah (Fauzi et al., 2022).

Tanggungjawab tersebut diwujud-kan melalui pembentukan UU PDP. Regulasi ini mengatur hak pemilik data, kewajiban pengelola data, mekanisme pemrosesan data, serta sanksi bagi pihak yang melakukan pelanggaran. Melalui UU PDP, negara berupaya menciptakan kepastian hukum dan meningkatkan keamanan pengelolaan data pribadi di berbagai sektor. Selain membentuk regulasi, negara juga memiliki kewajiban melakukan pengawasan dan penegakan hukum terhadap pelanggaran data pribadi. Pemerintah berperan dalam memastikan bahwa instansi maupun badan usaha yang mengelola data pribadi mematuhi ketentuan yang berlaku. Apabila terjadi pelanggaran, masyarakat berhak memperoleh perlindungan hukum, termasuk mengajukan tuntutan ganti rugi sesuai dengan mekanisme yang telah ditetapkan (Aqilah et al., 2024).

Perlindungan data pribadi pada dasarnya tidak hanya menempatkan negara sebagai pembentuk regulasi, tetapi juga sebagai penyelenggara tata kelola pemerintahan yang wajib menerapkan prinsip akuntabilitas (*accountability*) dalam setiap pemrosesan data pribadi. Prinsip tersebut menghendaki agar setiap instansi pemerintah mampu membuktikan bahwa seluruh tahapan pengumpulan, penyimpanan, penggunaan, pengungkap-an, hingga penghapusan data pribadi telah dilakukan sesuai dengan ketentuan peraturan perundang-undangan. Dengan demikian, akuntabilitas tidak hanya dimaknai sebagai kepatuhan administratif, melainkan juga sebagai kewajiban untuk menyediakan mekanisme audit, dokumen-tasi pemrosesan data, serta evaluasi keamanan sistem informasi secara berkala. Penerapan prinsip tersebut menjadi indikator penting dalam mengukur sejauh mana tanggung jawab negara telah dilaksanakan secara efektif dalam melindungi hak-hak subjek data pribadi (Solihin, 2023).

Lebih lanjut, perkembangan tata kelola data pribadi secara global menunjukkan bahwa efektivitas perlindungan data sangat dipengaruhi oleh keberadaan otoritas pengawas yang independen. Lembaga pengawas memiliki fungsi melakukan pengawasan terhadap kepatuhan pengendali data, menerima pengaduan masyarakat, melakukan investigasi, hingga menjatuhkan sanksi administratif apabila ditemukan pelanggaran. Keberadaan lembaga yang independen akan memperkuat prinsip *checks and balances* sehingga pengawasan terhadap instansi pemerintah tidak hanya dilakukan secara internal, tetapi juga melalui mekanisme pengawasan eksternal yang objektif. Dalam konteks Indonesia, penguatan fungsi pengawasan menjadi salah satu tantangan implementasi UU PDP mengingat efektivitas perlindungan data sangat bergantung pada koordinasi antarlembaga serta konsistensi penegakan hukum (Anggen Suari & Sasfarjana, 2023).

Aspek lain yang menjadi bagian penting dari tanggung jawab negara adalah penyediaan mekanisme pemulihan (*remedial protection*) bagi masyarakat yang menjadi korban pelanggaran data pribadi. UU PDP memberikan hak kepada subjek data untuk memperoleh informasi mengenai pemrosesan datanya, mengajukan keberatan atas penggunaan data, meminta perbaikan maupun penghapusan data tertentu, serta mengajukan gugatan apabila mengalami kerugian akibat pelanggaran data pribadi. Hak-hak tersebut menunjukkan bahwa perlindungan hukum tidak berhenti pada tahap pencegahan, melainkan juga mencakup penyediaan akses terhadap keadilan (*access to justice*) sebagai bentuk pertanggungjawaban negara. Keberadaan mekanisme pemulihan ini sekaligus mencerminkan bahwa perlindungan data pribadi merupakan bagian dari perlindungan hak konstitusional warga negara yang harus dijamin secara nyata dalam praktik penyelenggaraan pemerintahan. (Sane et al., 2025)

Selanjutnya, tanggung jawab negara juga diwujudkan melalui penerapan prinsip pencegahan (*preventive protection*). Dalam rezim perlindungan data modern, negara tidak cukup hanya memberikan sanksi setelah terjadi kebocoran data, tetapi wajib membangun sistem yang mampu mencegah terjadinya pelanggaran sejak awal. Bentuk perlindungan preventif tersebut meliputi penyusunan standar operasional pengamanan data, penerapan enkripsi, pengendalian akses berdasarkan tingkat kewenangan, pelaksanaan audit keamanan informasi secara berkala, hingga peningkatan kapasitas sumber daya manusia yang mengelola sistem elektronik. Pendekatan preventif ini merupakan implementasi dari prinsip kehati-hatian (*precautionary principle*) yang berkembang dalam tata kelola keamanan informasi modern. Oleh karena itu, efektivitas perlindungan data pribadi

tidak hanya diukur dari keberadaan aturan hukum, tetapi juga dari kesiapan institusi negara dalam mengantisipasi risiko kebocoran data sebelum kerugian dialami oleh masyarakat (Mahameru et al., 2024).

Dengan demikian, tanggung jawab negara dalam perlindungan data pribadi tidak hanya terbatas pada penyusunan peraturan perundang-undangan, tetapi juga mencakup pengawasan, penegakan hukum, dan pemberian jaminan perlindungan bagi warga negara. Keberadaan UU PDP menjadi langkah penting dalam memperkuat perlindungan hak privasi masyarakat di era digital.

B. Implikasi Tanggung Jawab Negara Terhadap Kebocoran Data Pemilih Tetap Di Komisi Pemilihan Umum Dalam Perspektif Hak Asasi Manusia

Kebocoran data DPT yang dikelola oleh KPU menimbulkan konsekuensi hukum yang serius karena data tersebut memuat informasi pribadi warga negara yang wajib dilindungi. Dalam perspektif hak asasi manusia, perlindungan data pribadi merupakan bagian dari hak atas privasi yang dijamin oleh konstitusi dan berbagai instrumen hak asasi manusia. Oleh karena itu, ketika terjadi kebocoran data DPT, negara tidak hanya menghadapi persoalan keamanan siber, tetapi juga potensi pelanggaran terhadap hak-hak dasar warga negara (Angraini K et al., 2024).

Sebagai penyelenggara pemilu, KPU memiliki kewajiban untuk menjamin kerahasiaan, integritas, dan keamanan data pemilih yang berada dalam penguasaannya. Kebocoran sekitar 240 juta data pemilih yang diduga berasal dari sistem KPU pada penyelenggaraan Pemilu 2024 menunjukkan adanya kelemahan dalam tata kelola dan sistem pengamanan data. Peristiwa tersebut menimbulkan kekhawatiran masyarakat karena data yang bocor berpotensi disalahgunakan untuk tindak kejahatan siber, pencurian identitas, maupun aktivitas lain yang merugikan pemilik data (Michael & Rasji, 2024).

Dari sudut pandang hak asasi manusia, kebocoran data pemilih dapat dikategorikan sebagai bentuk pelanggaran terhadap hak privasi warga negara. Hak atas privasi tidak hanya mencakup perlindungan terhadap kehidupan pribadi seseorang, tetapi juga hak untuk mengendalikan penggunaan informasi pribadi yang dimilikinya. Ketika data pribadi tersebar tanpa persetujuan pemilik data, maka hak tersebut menjadi terancam. Oleh karena itu, negara berkewajiban memastikan adanya perlindungan yang efektif terhadap seluruh data pribadi yang dikumpulkan dalam penyelenggaraan pelayanan publik, termasuk data pemilih (Angraini K et al., 2024).

Implikasi tanggung jawab negara atas kebocoran data DPT dapat dilihat dalam beberapa aspek. Pertama, negara berkewajiban melakukan investigasi secara menyeluruh untuk menemukan penyebab dan pihak yang bertanggung jawab atas kebocoran tersebut. Kedua, negara harus mengambil langkah pemulihan guna meminimalkan dampak yang dialami oleh masyarakat. Ketiga, negara wajib memperkuat sistem keamanan data agar kejadian serupa tidak terulang pada masa mendatang. Kegagalan dalam menjalankan kewajiban tersebut dapat menurunkan kepercayaan publik terhadap institusi penyelenggara pemilu maupun pemerintah secara umum (Angraini K et al., 2024).

Dalam kerangka UU PDP, KPU sebagai pengendali data memiliki tanggung jawab untuk menerapkan langkah-langkah teknis dan organisatoris yang memadai dalam melindungi data pemilih. Apabila terjadi kebocoran akibat kelalaian atau kegagalan dalam memenuhi kewajiban tersebut, maka dapat timbul konsekuensi hukum berupa sanksi administratif maupun bentuk pertanggung-jawaban lainnya sesuai ketentuan peraturan perundang-undangan. Penelitian mengenai pengamanan data oleh KPU bahkan menunjukkan bahwa kelemahan dalam perlindungan data pemilih dapat menimbulkan tanggung jawab hukum bagi lembaga tersebut (Hisbulloh, 2021).

Dengan demikian, kebocoran data pemilih tetap tidak hanya berdampak pada keamanan informasi, tetapi juga berkaitan langsung dengan pemenuhan dan perlindungan hak asasi manusia. Negara memiliki tanggung jawab untuk menjamin keamanan data pribadi warga negara melalui regulasi, pengawasan, penegakan hukum, dan pemulihan hak korban. Pelaksanaan tanggung jawab tersebut menjadi penting untuk menjaga kepercayaan masyarakat terhadap sistem demokrasi dan penyelenggaraan pemilu yang berintegritas (Angraini K et al., 2024).

KESIMPULAN DAN SARAN

Perlindungan data pribadi merupakan bagian yang tidak terpisahkan dari pemenuhan hak asasi manusia, khususnya hak atas privasi, sehingga negara memiliki kewajiban konstitusional untuk

menghormati, melindungi, dan memenuhi hak tersebut melalui regulasi yang memadai, tata kelola yang akuntabel, serta penegakan hukum yang efektif. Pengaturan mengenai tanggung jawab negara telah memperoleh landasan hukum yang cukup melalui Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta berbagai peraturan yang mengatur pengelolaan data dalam penyelenggaraan pemilu. Kerangka hukum tersebut menempatkan negara tidak hanya sebagai pembentuk regulasi, tetapi juga sebagai pengendali data yang wajib menerapkan prinsip akuntabilitas, keamanan, transparansi, dan perlindungan yang efektif terhadap setiap data pribadi yang dikelolanya.

Namun demikian, kebocoran Data Pemilih Tetap (DPT) pada Komisi Pemilihan Umum menunjukkan bahwa implementasi tanggung jawab negara belum berjalan secara optimal. Insiden tersebut memperlihatkan masih lemahnya sistem keamanan siber, tata kelola data, mekanisme pengawasan, serta respons terhadap insiden kebocoran data. Dari perspektif hak asasi manusia, kebocoran DPT tidak hanya menimbulkan risiko penyalahgunaan identitas dan kejahatan siber, tetapi juga merupakan bentuk ancaman terhadap hak atas privasi warga negara serta berpotensi mengurangi kepercayaan masyarakat terhadap penyelenggaraan pemilu dan institusi pemerintah. Kondisi tersebut menunjukkan bahwa keberadaan regulasi semata belum cukup apabila tidak disertai implementasi yang konsisten, pengawasan yang efektif, dan mekanisme pertanggungjawaban yang jelas.

Oleh karena itu, tanggung jawab negara dalam perlindungan data pribadi harus diwujudkan secara menyeluruh melalui penguatan tata kelola keamanan informasi, penerapan standar perlindungan data yang berbasis manajemen risiko, peningkatan kapasitas keamanan siber pada seluruh instansi publik, pembentukan mekanisme pengawasan yang independen dan efektif, serta penegakan sanksi terhadap setiap bentuk kelalaian maupun pelanggaran dalam pengelolaan data pribadi. Di samping itu, negara perlu menjamin adanya mekanisme pemulihan yang cepat, transparan, dan berkeadilan bagi subjek data yang dirugikan akibat kebocoran data. Dengan demikian, perlindungan data pribadi tidak hanya menjadi kewajiban administratif, tetapi merupakan manifestasi nyata dari tanggung jawab negara dalam menjamin hak asasi manusia, memperkuat kepastian hukum, serta membangun kepercayaan publik terhadap penyelenggaraan pemerintahan dan demokrasi digital di Indonesia.

DAFTAR PUSTAKA

Abdullah, Chairunnisa, et al. *Transformasi Digital Dan Hak Atas Privasi : Tinjauan Kritis Pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022 Di Era Big Data*. vol. 2, 2025.

Alfian Kusnaldi, M., Fadila Syani, N., & Yukiatiqa Afifah, dan. (2022). *Perlindungan Data Pribadi dalam Penyelenggaraan Pemilu: Tantangan dan Tawaran* (Vol. 7, Number 4).

Amiruddin, (2016). *Pengantar Metode Penelitian hukum* (9th ed.). Rajagrafindo.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Angraini K, Novita, et al. "PERLINDUNGAN HUKUM DATA PRIBADI DALAM PERSPEKTIF HAK ASASI MANUSIA." *Indonesian Journal of Legality of Law*, vol. 7, no. 1, Dec. 2024, pp. 46–51, https://doi.org/10.35965/ijlf.v7i1.5267.

Argiansyah, Hikmal Yusuf, et al. *Analisis Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia*. vol. 5, no. 1, 2024, pp. 61–75.

Aritonang, Lenny Maria, and Rara Handayani. *Analisis Hukum Terhadap Kebocoran Data Pribadi Dan Penyalahgunaan Identitas Dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. vol. 7, no. 5, 2025, pp. 3146–58.

Aqilah, Rosa, et al. *Jurnal Ilmiah Kutei Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. vol. 23, no. 2, 2024, pp. 158–72, https://doi.org/10.33369/jik.v23i2.34476.

Bua, Imanuel Toding, and Nur Isdah Idris. *Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024*. vol. 2, 2025, pp. 100–14.

Darmawan, Stephanie Priscilla. *Hak Konstitusional Atas Privasi Di Era Digital*. vol. 12, 2023, pp.

1019–25.
Fauzi, Elfian, et al. *Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. 2022.
Hakim, Lukman, and Nalom Kurniawan. "Developing Paradigm of Indonesian Human Rights Law Based on Human Rights Obligation." *Jurnal Konstitusi*, vol. 18, no. 4, 2021, pp. 869–97, https://doi.org/10.31078/jk1847.
Harisudin Noor, Rahman Mohammad. *Konstitusionalisme Digital,Privasi Dan Hak Asasi Manusia:Sebuah Tinjauan Yuridis Terhadap Kerangka Hukum Indonesia Dalam Konteks Internasional*. 2025.
Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, M. H. (2024). *IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA*.
Michael, and Rasji. *Analisis Yuridis Peristiwa Kebocoran Data Daftar Pemilih Tetap Dalam Penyelenggaraan Pemilihan Umum Tahun 2024*. 2024, https://doi.org/10.38035/jihhp
Jonaedi, (2024). *Metode Penelitian Hukum*. Kencana.
Kunto, Muhammad, and Tri Wibowo. *Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane Tanggung Jawab Komisi Pemilihan Umum Atas Kegagalan Pelindungan Data Pribadi Dalam Pemilihan Umum Tahun 2024*. vol. 2, no. 4, p. 88, https://doi.org/10.5281/zenodo.14008008.
Michael, and Rasji. *Analisis Yuridis Peristiwa Kebocoran Data Daftar Pemilih Tetap Dalam Penyelenggaraan Pemilihan Umum Tahun 2024*. 2024, https://doi.org/10.38035/jihhp.v4i4.
Milafebina, Rachel, and Amad Sudiro. *Bentuk Perlindungan Hukum Terhadap Data Pribadi Pengguna Pada Platform Digital Di Indonesia*. 2025, pp. 7740–50.
Mulyadi, Dedi, et al. *Implementasi Kebijakan Pemerintah Terhadap Pencegahan Kebocoran Data Pribadi Dalam Pelayanan Publik Berbasis Digital*. no. 1, 2026, pp. 1–15.
Nugraha, Dimas Aditya, et al. *Kebocoran Dat BPJS Kesehatan: Ancaman Terhadap Keamanan Informasi Publik Di Era Digital*. vol. 2, no. 3, 2021, pp. 4685–91.
Rusyda, Nabiha Khansa. *Perlindungan Hukum Erhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022*. 2025.
Sane, M., Sinambela, H., Eli Hutahaean, R., & Hutahaean dan Lasbok Marbun, L. (2025). IMPLEMENTASI REGULASI PERLINDUNGAN DATA PRIBADI DALAM LAYANAN DIGITAL DI INDONESIA: A SYSTEMATIC REVIEW IMPLEMENTATION OF PERSONAL DATA PROTECTION REGULATIONS IN DIGITAL SERVICES IN INDONESIA: A SYSTEMATIC REVIEW. In *Jurnal Hukum Lex Generalis* (Vol. 6, Number 12). https://jhlg.rewangrencang.com/
Seta Ari Yuwana, Muhammad Asti, et al. *Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) Andhika Pratama Adhi Surya M . Asif Nur Fauzi*. vol. 4, no. 156, 2025, pp. 31–37.
Solihin, F. (2023). ANALISA CAKUPAN HUKUM PENGELOLAAN PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA. *Politik Dan Pemerintahan*, *12*.
Tri Wibowo, Muhammad Kunto. *Tanggung Jawab Komisi Pemilihan Umum Atas Kegagalan Pelindungan Data Pribadi Dalam Pemilihan Umum Tahun 2024*. vol. 2, no. 4, 2024, pp. 88–95.
Utami, Tanti Kirana, et al. *Personal Data Breach Cases in Indonesia : Perspective Of Personal Data Protection Law*. no. 2, 2025, pp. 1–21.