Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
Vol. 5. No. 3. 2026

Tanggung Jawab Mutlak Pengendali Data Akibat Kebocoran Data Pribadi di Aplikasi Mypertamina

Mangaraja Gideon Silaen*, Men Wih Widiatno
Universitas Esa Unggul, Indonesia
Email: gideon.silaen@student.esaunggul.ac.id*, menwih@esaunggul.ac.id

Kata Kunci
Perlindungan Data Pribadi, Tanggungjawab Mutlak, Pengendali Data

Abstrak
Penelitian ini mengkaji penerapan prinsip tanggung jawab mutlak sebagai instrumen perlindungan hukum dalam rezim sanksi administratif Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kajian ini dilatarbelakangi oleh meningkatnya insiden kebocoran data pribadi di Indonesia, salah satunya kebocoran data pengguna aplikasi MyPertamina pada November 2022, yang menimbulkan kebutuhan akan mekanisme perlindungan hukum yang efektif bagi subjek data. Penelitian menggunakan pendekatan yuridis normatif melalui studi kepustakaan terhadap bahan hukum primer, sekunder, dan tersier, dengan analisis deskriptif-analitis terhadap norma UU PDP. Hasil penelitian menunjukkan bahwa UU PDP menempatkan pengendali data sebagai pihak yang memikul kewajiban preventif dan berkelanjutan dalam menjamin keamanan pemrosesan data pribadi. Dalam konteks kasus MyPertamina, penelitian ini menganalisis posisi pengendali data dalam kerangka UU PDP untuk memahami batas-batas pertanggungjawaban administratif apabila kebocoran data terjadi dalam ruang kendali sistem dan proses pemrosesan data. Penerapan prinsip tanggung jawab mutlak dalam ranah hukum administratif dipahami sebagai bentuk perlindungan hukum yang berorientasi pada pencegahan risiko, penguatan kepatuhan, dan perlindungan hak subjek data atas keamanan data pribadi.

Keywords
Personal Data Protection, Strict liability, Data Controller

Abstract
This study examines the application of strict liability as a legal protection mechanism within the administrative sanctions regime under Law Number 27 of 2022 on Personal Data Protection (PDP Law). The research is motivated by the increasing occurrence of personal data breaches in Indonesia, including the MyPertamina application data breach in November 2022, which highlights the need for effective legal protection for data subjects. This study employs a normative juridical approach through library research, analyzing primary, secondary, and tertiary legal materials using a descriptive-analytical method. The findings indicate that the PDP Law places data controllers under preventive and continuous obligations to ensure the security of personal data processing. In the context of the MyPertamina case, this study analyzes the position of the data controller within the PDP Law framework to understand the scope of administrative liability when a data breach occurs within the controller's system control and data processing activities. The application of strict liability in the administrative regime is conceptualized as a form of legal protection aimed at risk prevention, strengthening compliance, and safeguarding data subjects' rights.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong berbagai aktivitas masyarakat Indonesia beralih ke ruang digital, termasuk transaksi ekonomi, penyelenggaraan layanan publik, serta pengelolaan administrasi pemerintahan. Dalam proses digitalisasi

tersebut, data pribadi menjadi elemen yang tidak terpisahkan dari berbagai layanan berbasis sistem elektronik. Di sisi lain, intensitas pengumpulan dan pemrosesan data pribadi juga meningkatkan risiko pelanggaran privasi, peretasan sistem, dan penyalahgunaan data yang dapat menimbulkan kerugian bagi subjek data. Kondisi ini menuntut adanya kerangka hukum yang mampu memberikan pelindungan efektif atas data pribadi sebagai bagian dari hak asasi manusia.

Sebagai respons atas kebutuhan tersebut, pemerintah Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai dasar hukum nasional dalam pengaturan pelindungan data pribadi. UU PDP mengklasifikasikan data pribadi ke dalam data pribadi umum dan data pribadi yang bersifat spesifik, dengan tingkat pelindungan yang lebih ketat terhadap data pribadi yang bersifat spesifik karena berkaitan langsung dengan identitas fundamental individu serta berpotensi menimbulkan dampak serius apabila disalahgunakan (Rusyda, 2025). Pelindungan terhadap data pribadi tidak hanya dimaksudkan untuk mencegah kerugian material, tetapi juga untuk menjaga martabat individu dan kepercayaan publik terhadap penyelenggaraan layanan digital (Wiraguna et al., 2024).

Salah satu contoh kebocoran data pribadi yang terjadi di Indonesia adalah kebocoran data pengguna aplikasi MyPertamina pada November 2022. Peristiwa ini dilaporkan oleh berbagai media arus utama nasional yang mengungkap dugaan kebocoran data pengguna dalam jumlah besar, mencakup informasi identitas seperti Nomor Induk Kependudukan (NIK), data kontak, serta informasi penggunaan layanan subsidi bahan bakar minyak (CNN, 2022; Detik.com, 2022; Kompas.com, 2022). Laporan media teknologi menunjukkan bahwa data tersebut tersebar dalam bentuk basis data terstruktur yang mengindikasikan kebocoran berasal dari sistem pengelolaan data, bukan akibat kesalahan pengguna akhir (Gizmologi.id., 2022). Data yang dilaporkan bocor tersebut mencakup jenis data pribadi yang termasuk dalam kategori data pribadi yang bersifat spesifik atau setidaknya memiliki karakteristik yang memerlukan tingkat pelindungan lebih ketat berdasarkan UU PDP, sehingga berpotensi menimbulkan penyalahgunaan data pribadi dan pencurian identitas dalam skala luas.

Kasus MyPertamina tersebut menunjukkan bahwa kebocoran data pribadi di Indonesia bukanlah fenomena yang bersifat hipotetis, melainkan persoalan nyata yang berdampak langsung pada subjek data dan kepercayaan publik. Dalam konteks yang lebih luas, berbagai insiden kebocoran data di Indonesia memperlihatkan bahwa penegakan hukum pelindungan data pribadi masih menghadapi tantangan, khususnya ketika pertanggungjawaban hukum pengendali data dipahami melalui paradigma berbasis kesalahan (*fault-based liability*). Pendekatan ini menimbulkan kesulitan pembuktian karena kebocoran data umumnya bersifat teknis, kompleks, dan melibatkan asimetri informasi antara pengendali data dan subjek data, sehingga berpotensi melemahkan efektivitas sanksi administratif (Alatas & Djajaputra, 2026).

Di sisi lain, UU PDP menetapkan kewajiban pelindungan data pribadi yang bersifat preventif dan berkelanjutan bagi Pengendali Data. Pengendali Data ditempatkan sebagai pihak yang bertanggung jawab secara normatif atas pemenuhan kewajiban keamanan dan pengelolaan pemrosesan data pribadi, sebagai bagian dari upaya negara dalam menjamin hak atas privasi dan keamanan data subjek data (Mahameru et al., 2023). Oleh karena itu, kegagalan menjaga keamanan data baik yang disebabkan oleh kelemahan sistem, pengendalian internal, maupun faktor teknis lainnya dapat dipandang sebagai kegagalan pemenuhan kewajiban hukum tanpa harus terlebih dahulu dibuktikan adanya kesalahan subjektif (Afifah, 2024).

Pelindungan data pribadi dalam sistem elektronik menuntut adanya pengaturan hukum yang menempatkan Pengendali Data sebagai pihak yang bertanggung jawab secara aktif atas keamanan dan tata kelola pemrosesan data, khususnya dalam ekosistem layanan publik digital (Kurdi & Cahyono, 2024). Dalam konteks inilah prinsip tanggung jawab mutlak (strict liability) dalam ranah hukum sanksi administratif menjadi relevan sebagai instrumen hukum yang bersifat objektif dan berorientasi pada pencegahan risiko.

Pendekatan pertanggungjawaban administratif yang bersifat objektif tersebut juga sejalan dengan perkembangan hukum pelindungan data pribadi di tingkat internasional. General Data Protection Regulation (GDPR) Uni Eropa menempatkan pengendali data sebagai pihak yang bertanggung jawab atas kepatuhan dan keamanan pemrosesan data pribadi melalui kewajiban teknis dan organisasi yang bersifat preventif, dengan mekanisme sanksi administratif yang pada prinsipnya tidak mensyaratkan pembuktian kesalahan subjektif dari pengendali data (Simanjuntak, 2024). Model pertanggungjawaban ini menunjukkan bahwa efektivitas pelindungan data pribadi bertumpu pada standar kepatuhan dan pengelolaan risiko yang melekat pada posisi pengendali data, bukan semata-mata pada pembuktian unsur kesalahan (Dresch & Júnior, 2024; Wilantara et al., 2024). Di tingkat nasional, arah kebijakan serupa tercermin dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024, khususnya melalui Pasal 40A yang mendorong penyelenggaraan sistem elektronik yang akuntabel, aman, dan bertanggung jawab melalui mekanisme pengawasan dan sanksi administratif. Namun demikian, dalam konteks pelindungan data pribadi, UU PDP tetap berlaku sebagai lex specialis yang menjadi dasar utama pengaturan hak, kewajiban, dan pertanggungjawaban pengendali data.

Beberapa penelitian terdahulu telah mengkaji aspek pertanggungjawaban hukum dalam pelindungan data pribadi. Hasan (2024) menganalisis tanggung jawab pelaku usaha terhadap perlindungan data pribadi konsumen dan menekankan perlunya mekanisme pertanggungjawaban yang tidak bertumpu pada pembuktian kesalahan, namun tidak mengkaji penerapan prinsip tanggung jawab mutlak dalam ranah sanksi administratif UU PDP. Rumbruren dan Watofa (2025) mengkaji tanggung jawab penyelenggara sistem elektronik dalam kebocoran data dan menemukan bahwa kompleksitas teknis serta asimetri informasi menyebabkan mekanisme berbasis kesalahan tidak efektif, sehingga diperlukan pendekatan pertanggungjawaban yang lebih objektif, namun belum mengaitkannya secara sistematis dengan konstruksi tanggung jawab mutlak dalam hukum administrasi. Simanjuntak (2024) melakukan studi komparatif antara UU PDP dan GDPR, menunjukkan bahwa GDPR menempatkan prinsip akuntabilitas sebagai fondasi pertanggungjawaban dengan sanksi administratif yang tidak mensyaratkan pembuktian kesalahan subjektif, namun belum mengkaji penerapan prinsip tersebut dalam kasus konkret kebocoran data di Indonesia pasca berlakunya UU PDP.

Penelitian sebelumnya masih terbatas pada aspek normatif kewajiban pengendali data secara umum, belum mengkaji konstruksi dan penerapan prinsip tanggung jawab mutlak dalam rezim sanksi administratif UU PDP pasca berlakunya undang-undang. Belum ada penelitian yang menganalisis secara sistematis hubungan antara norma kewajiban pengendali data dengan mekanisme sanksi administratif sebagai manifestasi prinsip tanggung jawab mutlak, menggunakan kasus kebocoran data MyPertamina sebagai studi kasus normatif, serta

membedakan secara tegas konstruksi strict liability dalam hukum administrasi dengan konsep serupa dalam hukum perdata dan pidana. Penelitian sebelumnya masih terbatas pada aspek normatif kewajiban pengendali data secara umum, belum mengkaji konstruksi dan penerapan prinsip tanggung jawab mutlak dalam rezim sanksi administratif UU PDP pasca berlakunya undang-undang. Belum ada penelitian yang menganalisis secara sistematis hubungan antara norma kewajiban pengendali data dengan mekanisme sanksi administratif sebagai manifestasi prinsip tanggung jawab mutlak, menggunakan kasus kebocoran data MyPertamina sebagai studi kasus normatif, serta membedakan secara tegas konstruksi strict liability dalam hukum administrasi dengan konsep serupa dalam hukum perdata dan pidana.

Permasalahan utama dalam pelindungan data pribadi tidak hanya terletak pada ketersediaan norma hukum, tetapi juga pada konstruksi pertanggungjawaban yang digunakan dalam penegakan sanksi administratif terhadap pengendali data. Oleh karena itu, penelitian ini difokuskan pada pengkajian penerapan prinsip tanggung jawab mutlak pengendali data berdasarkan Undang-Undang Perlindungan Data Pribadi. Kasus kebocoran data MyPertamina dalam penelitian ini diposisikan sebagai konteks untuk mengkaji penerapan norma UU PDP secara normatif, khususnya dalam memahami konstruksi tanggung jawab pengendali data, tanpa dimaksudkan untuk menilai atau menetapkan adanya kesalahan faktual dari pihak tertentu.

Berdasarkan hasil dari pemaparan latar belakang masalah di atas, penelitian ini bertujuan menganalisis konstruksi normatif prinsip tanggung jawab mutlak dalam UU PDP, mengkaji penerapannya dalam kasus kebocoran data MyPertamina, dan merumuskan pemahaman konseptual mengenai batasan tanggung jawab mutlak administratif yang berbeda dengan rezim perdata dan pidana. Penelitian ini memberikan manfaat teoritis bagi pengembangan ilmu hukum pelindungan data pribadi dan hukum administrasi, serta manfaat praktis bagi lembaga pengawas dalam merumuskan tata cara sanksi administratif, bagi pengendali data dalam memahami tanggung jawabnya, dan bagi masyarakat dalam memahami mekanisme pelindungan hukum jika terjadi kebocoran data.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif (Muhaimin, 2020). Pendekatan ini dipilih untuk mengkaji norma-norma hukum yang mengatur penerapan prinsip tanggung jawab mutlak dalam rezim pelindungan data pribadi, khususnya tanggung jawab pengendali data atas kebocoran data pribadi, serta untuk menganalisis konstruksi tanggung jawab hukum PT Pertamina sebagai pengendali data dalam pengelolaan aplikasi MyPertamina berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

Pendekatan perundang-undangan (statute approach) digunakan untuk menelaah secara sistematis ketentuan dalam UU PDP, meliputi asas pelindungan dan pertanggungjawaban, pengertian serta klasifikasi data pribadi, kewajiban pengendali data dalam menjaga keamanan pemrosesan data, kewajiban pelaporan insiden kebocoran data, serta mekanisme sanksi administratif. Pendekatan ini dimaksudkan untuk membangun pemahaman normatif mengenai konstruksi dan karakter tanggung jawab pengendali data dalam rezim hukum pelindungan data pribadi, dengan menempatkan undang-undang sebagai sumber utama dalam analisis norma dan sistematika pengaturan (Marzuki, 2017).

Bahan hukum yang digunakan terdiri atas bahan hukum primer, meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024. Selain itu, Undang-Undang Nomor 32 Tahun 2009 tentang Perlindungan dan Pengelolaan Lingkungan Hidup digunakan secara terbatas sebagai rujukan konseptual untuk memahami karakter tanggung jawab mutlak dalam ranah hukum sanksi administratif di Indonesia. Bahan hukum sekunder meliputi buku teks hukum, artikel jurnal ilmiah nasional dan internasional, serta dokumen akademik yang relevan dengan hukum perlindungan data pribadi, hukum administrasi, dan perkembangan standar pelindungan data di tingkat internasional, termasuk regulasi perlindungan data Uni Eropa (General Data Protection Regulation/GDPR) sebagai rujukan konseptual Bahan hukum tersier mencakup kamus hukum, ensiklopedia hukum, serta sumber penunjang lainnya.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu penelusuran sistematis terhadap bahan hukum primer, sekunder, dan tersier yang relevan dengan objek penelitian (Soekanto & Mamudji, 2018). Penelitian ini juga menggunakan kasus kebocoran data aplikasi MyPertamina tahun 2022 sebagai ilustrasi aplikatif, yang dimanfaatkan untuk menunjukkan penerapan norma UU PDP dalam konteks faktual, tanpa dimaksudkan untuk menilai atau membuktikan aspek teknis kebocoran data secara empiris.

Analisis bahan hukum dilakukan secara kualitatif dengan pendekatan deskriptif-analitis, melalui penafsiran sistematis, historis, dan teleologis terhadap norma hukum yang relevan. Analisis ini diarahkan untuk membangun argumentasi normatif mengenai penerapan prinsip tanggung jawab mutlak dalam ranah hukum sanksi administratif UU PDP serta implikasinya terhadap tanggung jawab pengendali data dalam kasus kebocoran data pribadi.

HASIL DAN PEMBAHASAN

A. Penerapan Prinsip Tanggung Jawab Mutlak Pengendali Data dalam UU Pelindungan Data Pribadi

1. Norma Dasar UU PDP dan Urgensi Pelindungan Data Pribadi

Pelindungan data pribadi merupakan bagian integral dari pelindungan hak asasi manusia, khususnya hak atas rasa aman dan hak atas perlindungan diri pribadi sebagaimana dijamin dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Perkembangan teknologi digital yang memungkinkan pengumpulan, pengolahan, dan pertukaran data dalam skala besar telah meningkatkan risiko penyalahgunaan data pribadi, sehingga menuntut kehadiran instrumen hukum yang memberikan perlindungan yang efektif dan berorientasi pada kepentingan subjek data. Dalam konteks tersebut, UU PDP hadir sebagai respons normatif negara untuk menjamin hak konstitusional warga negara di ruang digital.

Secara teoretis, pelindungan data pribadi dapat dipahami melalui teori pelindungan hukum sebagaimana dikemukakan oleh Philipus M. Hadjon, yang memandang pelindungan hukum sebagai upaya negara untuk memberikan jaminan kepastian dan rasa aman kepada warga negara melalui instrumen hukum yang bersifat preventif dan represif (Hadjon, 2011). Pelindungan hukum preventif bertujuan mencegah terjadinya pelanggaran hak melalui pengaturan norma dan kewajiban yang jelas, sedangkan pelindungan hukum represif berfungsi

untuk memberikan pemulihan ketika pelanggaran telah terjadi. Dalam konteks pelindungan data pribadi, dimensi preventif menjadi sangat penting karena risiko kebocoran data bersifat laten, masif, dan sulit dipulihkan sepenuhnya setelah terjadi.

Teori pelindungan hukum Hadjon menekankan bahwa hukum harus memberikan perlindungan yang efektif bagi pihak yang berada dalam posisi lemah secara struktural. Dalam pemrosesan data pribadi, subjek data berada pada posisi yang asimetris dibandingkan dengan Pengendali Data, karena tidak memiliki kendali atas sistem, infrastruktur, maupun mekanisme pengamanan data. Sebaliknya, Pengendali Data memiliki kekuasaan faktual dan teknis atas seluruh siklus pemrosesan data pribadi. Oleh karena itu, pelindungan hukum yang efektif menuntut pembebanan kewajiban dan tanggung jawab yang lebih besar kepada pihak yang menguasai sumber risiko. Konstruksi ini sejalan dengan asas pelindungan, asas kehati-hatian, dan asas pertanggungjawaban sebagaimana diatur dalam Pasal 3 huruf a, e, dan g UU PDP, yang mengharuskan Pengendali Data untuk secara aktif mengantisipasi risiko serta bertanggung jawab atas setiap konsekuensi yang timbul dari pemrosesan data pribadi.

Urgensi pelindungan data pribadi semakin menguat apabila dikaitkan dengan karakter data pribadi yang bersifat sensitif, bernilai ekonomi, dan mudah disalahgunakan. Dalam praktiknya, subjek data tidak memiliki kapasitas teknis maupun akses terhadap informasi internal sistem elektronik untuk menilai apakah Pengendali Data telah menerapkan standar keamanan yang memadai. Kondisi ini menyebabkan mekanisme pelindungan hukum yang bertumpu pada pembuktian kesalahan subjektif menjadi tidak efektif, karena beban pembuktian justru diletakkan pada pihak yang paling dirugikan dan paling lemah posisinya (Hasan, 2024; Rofiq & Pujiyono, 2022).

Dalam kerangka teori pelindungan hukum, penerapan prinsip tanggung jawab mutlak (strict liability) dalam UU PDP harus dipahami sebagai konstruksi pertanggungjawaban administratif yang berdiri terpisah dari rezim pertanggungjawaban perdata berdasarkan perbuatan melawan hukum. Berbeda dengan tanggung jawab perdata yang mensyaratkan pembuktian unsur kesalahan, kerugian, dan hubungan kausalitas, tanggung jawab mutlak administratif dalam UU PDP berorientasi pada pengendalian risiko dan pemenuhan kewajiban normatif oleh Pengendali Data. Konstruksi ini sejalan dengan teori pelindungan hukum yang menempatkan hukum administrasi sebagai instrumen preventif dan korektif untuk melindungi kepentingan publik (Baldwin et al., 2011), terutama dalam situasi asimetri kendali dan kompleksitas teknis yang melekat pada pemrosesan data pribadi. Oleh karena itu, strict liability dalam UU PDP tidak dimaksudkan untuk menggantikan atau menghapus rezim tanggung jawab perdata, melainkan berfungsi sebagai mekanisme pelindungan hukum administratif guna memastikan kepatuhan, akuntabilitas, dan keamanan pemrosesan data pribadi, sebagaimana tercermin dalam asas pelindungan, kehati-hatian, dan pertanggungjawaban dalam Pasal 3 UU PDP.

Berdasarkan kerangka teoretis tersebut, UU PDP dirancang untuk memperkuat pelindungan hukum subjek data dengan menitikberatkan pada pemenuhan kewajiban normatif Pengendali Data, bukan semata-mata pada pencarian kesalahan individual. Pendekatan ini mencerminkan pergeseran orientasi pelindungan hukum dari model reaktif menuju model preventif dan berbasis risiko, sebagaimana dianjurkan dalam teori pelindungan hukum administrasi modern (Hadjon, 2011). Dengan demikian, pembahasan selanjutnya akan mengkaji bagaimana paradigma pelindungan hukum tersebut melandasi pergeseran dari

pertanggungjawaban berbasis kesalahan (fault-based liability) menuju penerapan prinsip tanggung jawab mutlak dalam rezim pelindungan data pribadi.

2. Pergeseran Paradigma Dari Fault-based liability Ke Strict liability Dalam Pelindungan Data Pribadi

Prinsip tanggung jawab mutlak (strict liability) pada mulanya dikenal dalam ranah hukum hukum yang berorientasi pada pengendalian risiko, khususnya dalam bidang-bidang yang melibatkan kegiatan berbahaya, kompleks, dan berpotensi menimbulkan kerugian luas bagi kepentingan publik. Dalam perkembangannya, prinsip ini tidak hanya diterapkan dalam konteks perdata, seperti dalam hukum lingkungan hidup, tetapi juga mengalami adaptasi dalam hukum administrasi modern sebagai instrumen penegakan kewajiban normatif dan pengendalian risiko. Dalam konteks pelindungan data pribadi, strict liability dipahami bukan sebagai penghapusan seluruh bentuk pertanggungjawaban berbasis kesalahan, melainkan sebagai mekanisme hukum untuk memastikan kepatuhan terhadap kewajiban pelindungan data yang secara faktual berada di bawah kendali Pengendali Data.

Dalam ranah hukum pelindungan data pribadi, kompleksitas teknologi informasi, asimetri kendali antara Pengendali Data dan subjek data, serta besarnya potensi dampak kebocoran data menjadikan pendekatan pertanggungjawaban berbasis kesalahan (fault-based liability) kurang memadai sebagai instrumen pelindungan hukum yang efektif. Subjek data berada dalam posisi yang lemah untuk membuktikan sebab-sebab teknis kebocoran, konfigurasi sistem, maupun kelalaian organisatoris yang bersifat internal, karena penguasaan atas sistem elektronik dan informasi pemrosesan data sepenuhnya berada pada Pengendali Data. Oleh karena itu, pertanggungjawaban dalam hukum administrasi pelindungan data diarahkan pada pemenuhan kewajiban normatif, bukan pada pembuktian kesalahan subjektif secara rinci (Rumbruren & Watofa, 2025).

Pendekatan tersebut sejalan dengan perkembangan hukum pelindungan data internasional, khususnya dalam General Data Protection Regulation (GDPR), yang menempatkan prinsip akuntabilitas sebagai fondasi utama pertanggungjawaban pengendali data. Melalui prinsip ini, pengendali data tidak hanya diwajibkan untuk mematuhi ketentuan pelindungan data, tetapi juga harus mampu menunjukkan dan membuktikan kepatuhan tersebut kepada otoritas yang berwenang (Wiraguna et al., 2024). Dengan demikian, sanksi administratif dapat dijatuhkan berdasarkan kegagalan pemenuhan kewajiban normatif, tanpa mensyaratkan pembuktian adanya kesalahan subjektif, niat jahat, atau kelalaian teknis tertentu. Dalam konteks hukum nasional, prinsip tersebut menemukan relevansinya dalam UU PDP, khususnya melalui perumusan kewajiban Pengendali Data yang bersifat komprehensif dan berlapis. Kewajiban untuk menjamin keamanan data, menerapkan langkah pengamanan teknis dan organisatoris, serta memastikan akuntabilitas pemrosesan data menunjukkan bahwa UU PDP mengadopsi pendekatan pengendalian risiko yang menjadi karakter utama strict liability administratif. Kegagalan pelindungan data, dalam kerangka ini, dipahami sebagai kegagalan pemenuhan kewajiban normatif, bukan semata-mata sebagai peristiwa teknis yang netral.

Dalam kerangka teori pelindungan hukum, penerapan prinsip tanggung jawab mutlak dalam UU PDP harus dipahami sebagai konstruksi pertanggungjawaban administratif yang berdiri terpisah dari rezim pertanggungjawaban perdata berdasarkan perbuatan melawan hukum maupun pertanggungjawaban pidana. Berbeda dengan pertanggungjawaban perdata yang mensyaratkan pembuktian unsur kesalahan, kerugian, dan hubungan kausalitas, tanggung

jawab mutlak administratif dalam UU PDP berorientasi pada pencegahan risiko dan pemulihan tertib hukum melalui penegakan kewajiban normatif. Oleh karena itu, penerapan strict liability dalam UU PDP tidak dimaksudkan untuk menggantikan atau menghapus rezim pertanggungjawaban hukum lainnya, melainkan berfungsi sebagai mekanisme pelindungan hukum administratif guna menjamin kepatuhan, akuntabilitas, dan keamanan pemrosesan data pribadi, sebagaimana tercermin dalam asas pelindungan, kehati-hatian, dan pertanggungjawaban dalam Pasal 3 UU PDP.

Sejalan dengan konstruksi tersebut, pembuktian dalam pertanggungjawaban administratif berdasarkan UU PDP tidak diarahkan pada kesalahan subjektif atau pembuktian teknis terjadinya kebocoran data secara rinci sebagaimana dikenal dalam rezim pidana atau perdata. Fokus pertanggungjawaban administratif terletak pada terpenuhinya atau tidaknya kewajiban normatif Pengendali Data sebagaimana diatur dalam UU PDP. Dengan demikian, keberadaan indikasi kegagalan pelindungan data dalam ruang publik telah cukup untuk mengaktifkan mekanisme evaluasi kepatuhan dan potensi pengenaan sanksi administratif, tanpa menuntut pembuktian kesalahan sebagaimana dalam perbuatan melawan hukum. Pola ini secara fungsional menyerupai pembalikan beban pembuktian, namun secara konseptual merupakan konsekuensi logis dari prinsip akuntabilitas dan pengendalian risiko dalam hukum administrasi, bukan penerapan pembuktian terbalik dalam arti pidana atau perdata.

3. Konstruksi Norma Kewajiban Pengendali Data Pribadi dalam UU PDP sebagai Dasar Pertanggung-jawaban Administratif

Kewajiban Pengendali Data Pribadi dalam UU PDP dirumuskan secara komprehensif untuk memastikan pelindungan hak subjek data melalui pemrosesan data yang sah, aman, dan akuntabel. Norma kewajiban tersebut secara sistematis tercermin dalam Pasal 35 sebagai norma induk, yang kemudian dielaborasi lebih lanjut melalui kewajiban teknis, prosedural, dan akuntabilitas dalam Pasal 16, Pasal 46, dan Pasal 47 UU PDP. Kewajiban tersebut bersifat preventif karena ditujukan untuk mencegah terjadinya kegagalan pelindungan data, dan bersifat proaktif karena mewajibkan Pengendali Data untuk bertindak sebelum dan segera setelah terjadinya pelanggaran.

Pasal 35 UU PDP berfungsi sebagai norma induk yang menetapkan standar kepatuhan normatif dalam seluruh siklus pemrosesan data pribadi oleh Pengendali Data, termasuk prinsip keabsahan, transparansi, keamanan, dan pertanggungjawaban. Norma ini bersifat substantif dan prinsipil karena menetapkan standar kepatuhan normatif yang harus dipenuhi dalam seluruh siklus pemrosesan data pribadi. Dengan demikian, setiap penyimpangan dari prinsip-prinsip tersebut (termasuk kegagalan menjamin keamanan data) secara yuridis telah merupakan pelanggaran kewajiban, tanpa terlebih dahulu mensyaratkan pembuktian kesalahan subjektif Pengendali Data.

Kewajiban substantif dalam Pasal 35 tersebut diperkuat oleh Pasal 16 UU PDP yang mengatur kewajiban preventif Pengendali Data untuk menerapkan langkah-langkah pengamanan teknis dan organisatoris guna melindungi data pribadi dari kebocoran, akses tidak sah, atau penyalahgunaan. Pasal ini menempatkan keamanan data sebagai kewajiban aktif (active duty of care), sehingga kegagalan sistem pengamanan secara normatif dapat dipahami sebagai indikator tidak terpenuhinya kewajiban pelindungan data pribadi, bukan sekadar risiko teknis (Hasan, 2024).

Selain itu, Pasal 46 UU PDP mengatur kewajiban proaktif dan korektif yang bersifat reaktif, yakni kewajiban Pengendali Data untuk memberitahukan kegagalan pelindungan data pribadi kepada subjek data dan lembaga pengawas dalam jangka waktu tertentu. Norma ini berfungsi sebagai instrumen transparansi dan akuntabilitas, serta menegaskan bahwa kegagalan pelindungan data merupakan peristiwa hukum yang menuntut pertanggungjawaban administratif, bukan semata-mata peristiwa teknis yang menunggu pembuktian kesalahan.

Selanjutnya, Pasal 47 UU PDP menegaskan kewajiban akuntabilitas struktural Pengendali Data atas seluruh proses pemrosesan data pribadi yang berada dalam penguasaannya. Norma ini menempatkan tanggung jawab pada pihak yang secara faktual dan yuridis mengendalikan sistem, sehingga beban pembuktian kepatuhan secara normatif berada pada Pengendali Data. Dalam konteks ini, kegagalan pelindungan data dapat dipahami sebagai kegagalan pemenuhan kewajiban akuntabilitas, terlepas dari ada atau tidaknya kesalahan subjektif.

Meskipun norma kewajiban Pengendali Data telah dirumuskan secara jelas dan berlapis, penegakannya akan kehilangan efektivitas apabila masih bertumpu pada paradigma fault-based liability yang mensyaratkan pembuktian kesalahan. Asimetri informasi, kompleksitas teknis sistem elektronik, serta keterbatasan akses subjek data terhadap bukti internal Pengendali Data menunjukkan bahwa pendekatan berbasis kesalahan tidak sepenuhnya memadai. Kondisi ini menegaskan urgensi penerapan prinsip tanggung jawab mutlak administratif sebagai mekanisme penegakan kewajiban Pengendali Data yang lebih adaptif terhadap risiko kebocoran data pribadi.

4. Tanggung Jawab Mutlak sebagai Konstruksi Normatif Sanksi Administratif dalam UU PDP

Prinsip tanggung jawab mutlak dalam UU PDP menemukan manifestasi normatif utamanya melalui mekanisme sanksi administratif sebagaimana diatur dalam Pasal 57 UU PDP. Sanksi administratif yang meliputi peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, hingga pengenaan denda administratif, dirancang sebagai instrumen korektif dan preventif untuk memulihkan tertib hukum serta mencegah terulangnya pelanggaran kewajiban pelindungan data pribadi. Dalam konteks ini, penjatuhan sanksi administratif tidak mensyaratkan pembuktian kesalahan subjektif, karena fokus penegakan hukum diarahkan pada kegagalan pemenuhan kewajiban normatif oleh Pengendali Data Pribadi (Diah & Wiraguna, 2025).

Konstruksi tersebut sejalan dengan karakter hukum administrasi modern yang menempatkan kepatuhan dan pengendalian risiko sebagai tujuan utama penegakan hukum. Dalam rezim pelindungan data pribadi, tanggung jawab mutlak administratif berfungsi untuk mengatasi kesenjangan perlindungan hukum yang timbul akibat asimetri informasi dan kompleksitas teknis pemrosesan data pribadi. Subjek data secara struktural berada dalam posisi yang lemah untuk membuktikan sebab-sebab teknis kebocoran data, sehingga kegagalan pelindungan data dipahami sebagai pelanggaran normatif yang berdiri sendiri dan cukup untuk mengaktifkan sanksi administratif, tanpa perlu pembuktian kesalahan moral atau teknis secara rinci (Hasan, 2024).

Penerapan tanggung jawab mutlak administratif dalam UU PDP juga tidak berdiri sendiri, melainkan diperkuat oleh kerangka pengaturan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan

Undang-Undang Nomor 1 Tahun 2024. Pasal 40A UU ITE memberikan kewenangan kepada pemerintah untuk menjamin terselenggaranya sistem elektronik yang andal, aman, dan bertanggung jawab, serta untuk memerintahkan Penyelenggara Sistem Elektronik (PSE) melakukan penyesuaian atau tindakan tertentu guna mencegah dan menanggulangi pelanggaran. Ketentuan ini menegaskan bahwa rezim hukum siber Indonesia secara eksplisit mengakui peran sanksi administratif sebagai instrumen utama pengendalian risiko dan penegakan kepatuhan, terlepas dari pembuktian kesalahan subjektif.

Dalam hubungan antara UU PDP dan UU ITE, mekanisme sanksi administratif tersebut bersifat saling melengkapi. UU PDP berfungsi sebagai lex specialis dalam pelindungan data pribadi, khususnya dalam menetapkan kewajiban Pengendali Data dan konsekuensi hukum atas kegagalan pelindungan data, termasuk melalui Pasal 35 yang menegaskan tanggung jawab Pengendali Data atas seluruh pemrosesan data pribadi dalam penguasaannya. Sementara itu, UU ITE menyediakan kerangka umum pengawasan dan pengendalian terhadap Penyelenggara Sistem Elektronik melalui kewenangan administratif negara. Dengan demikian, ketika terjadi kegagalan pelindungan data pribadi dalam suatu sistem elektronik, tanggung jawab mutlak administratif dapat diterapkan berdasarkan UU PDP, dengan dukungan kewenangan pengawasan dan penindakan administratif sebagaimana diatur dalam Pasal 40A UU ITE.

Dari perspektif asas pelindungan dan asas pertanggungjawaban sebagaimana diatur dalam Pasal 3 UU PDP, integrasi antara sanksi administratif UU PDP dan kewenangan administratif UU ITE menegaskan bahwa pelindungan data pribadi bukan semata-mata isu privat, melainkan bagian dari kepentingan publik dalam menjaga keamanan dan kepercayaan masyarakat terhadap ekosistem digital. Oleh karena itu, penerapan tanggung jawab mutlak administratif merupakan instrumen kunci untuk memastikan bahwa Pengendali Data dan Penyelenggara Sistem Elektronik bertindak secara akuntabel dan proaktif dalam mengelola risiko kebocoran data pribadi, sekaligus menjadi dasar normatif untuk menilai pertanggungjawaban dalam kasus konkret kebocoran data pribadi.

Dengan demikian berdasarkan pembahasan tersebut, dapat disimpulkan bahwa prinsip tanggung jawab mutlak administratif dalam UU PDP merupakan bagian integral dari konstruksi perlindungan hukum data pribadi yang berorientasi pada pengendalian risiko dan pemenuhan kewajiban normatif oleh Pengendali Data. Prinsip ini bekerja dalam ranah hukum administrasi dengan menempatkan kegagalan pemenuhan kewajiban pelindungan data sebagai dasar pertanggungjawaban normatif, tanpa mensyaratkan pembuktian adanya kesalahan subjektif (Salsabila & Wiraguna, 2025)

Penerapan tanggung jawab mutlak administratif tersebut tidak dimaksudkan untuk menggantikan maupun meniadakan unsur kesalahan dalam rezim hukum perdata, khususnya dalam konstruksi perbuatan melawan hukum yang mensyaratkan adanya kesalahan. Sebaliknya, prinsip strict liability dalam UU PDP berfungsi sebagai mekanisme perlindungan hukum publik yang berdiri secara otonom dari pertanggungjawaban perdata dan pidana, guna menjamin efektivitas pelindungan hak subjek data melalui instrumen sanksi administratif.

B. Tanggung Jawab Hukum PT Pertamina sebagai Pengendali Data Pribadi dalam Kasus Kebocoran Data Aplikasi MyPertamina Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

1. Latar Belakang Fakta Kebocoran Data MyPertamina Pasca Berlakunya UU PDP dan Penetapan Status Pengendali Data

Informasi mengenai kasus kebocoran data pada aplikasi MyPertamina yang terjadi pada November 2022 merupakan salah satu peristiwa signifikan yang menguji efektivitas UU PDP dalam tahap awal implementasinya setelah diundangkan. Aplikasi MyPertamina yang diluncurkan oleh PT Pertamina (Persero) untuk memfasilitasi registrasi subsidi bahan bakar minyak (BBM) dan pembayaran non-tunai, memerlukan verifikasi identitas pengguna melalui integrasi dengan basis data Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil), termasuk Nomor Induk Kependudukan (NIK). Kebocoran ini terjadi hanya satu bulan setelah pengundangan UU PDP pada 17 Oktober 2022, sehingga menjadi tolak ukur dini bagi kemampuan regulasi baru ini dalam menangani insiden siber di sektor energi dan layanan publik. Insiden ini tidak hanya menimbulkan kekhawatiran privasi individu, tetapi juga menyoroti kerentanan integrasi data nasional, di mana data pribadi warga yang bersifat wajib dan sensitif dapat dieksploitasi untuk tujuan kriminal atau manipulasi subsidi.

Kebocoran tersebut, sebagaimana diberitakan secara luas oleh media arus utama, diduga melibatkan sekitar 44 juta data pengguna, termasuk nama lengkap, NIK, alamat email, nomor telepon, serta informasi terkait subsidi BBM (CNN, 2022; Detik.com, 2022; Kompas.com, 2022). Pelaku yang mengklaim diri sebagai hacker dengan nama Bjorka menyebarkan sampel data melalui forum online, dengan file bocor berupa database dump berformat CSV berukuran 6 GB saat terkompresi dan 30 GB saat tidak terkompresi, mencakup total sekitar 44.237.264 rekaman pengguna (Gizmologi.id., 2022). Karakteristik file ini menunjukkan bahwa kebocoran berasal dari sisi server internal aplikasi, bukan kesalahan pengguna individu. Meskipun Pertamina membantah kebocoran massal dan menyatakan bahwa data bocor hanyalah sampel terbatas, investigasi bersama dengan Telkom dan Kementerian Komunikasi dan Digital (Komdigi, dahulu Kominfo) mengonfirmasi adanya akses tidak sah, meskipun tidak ada rilis resmi mengenai jumlah pasti data yang terdampak. Respons Pertamina dalam ruang publik pada saat itu berupa klarifikasi dan pernyataan evaluasi sistem keamanan, tanpa adanya kompensasi langsung atau transparansi penuh kepada pengguna terdampak, yang memperburuk hilangnya kepercayaan masyarakat terhadap layanan digital BUMN.

Fakta kasus ini semakin kompleks karena keterkaitannya dengan program subsidi BBM nasional, di mana data NIK sebagai identitas unik warga menjadi kunci verifikasi eligibilitas. Kebocoran semacam ini tidak hanya berpotensi memicu penipuan identitas dan pengambilalihan akun, tetapi juga manipulasi data subsidi yang dapat merugikan anggaran negara. Hingga akhir 2025, kasus ini belum berujung pada sanksi administratif tegas dari lembaga pengawas, meskipun UU PDP telah memberikan mandat untuk penegakan cepat, sehingga menekankan urgensi evaluasi tanggung jawab pengendali data seperti PT Pertamina dalam konteks hukum siber nasional.

Peristiwa ini menjadi perhatian serius karena terjadi setelah UU PDP diundangkan, sehingga seluruh kewajiban Pengendali Data Pribadi telah mengikat secara penuh pada saat informasi kebocoran tersebut diketahui publik. Pasca pemberitaan tersebut, PT Pertamina

(Persero) menyampaikan klarifikasi resmi yang menyatakan bahwa tidak ditemukan bukti kebocoran data dari sistem internal MyPertamina dan bahwa data pengguna tetap aman. Selain itu, Pertamina menyebutkan telah melakukan koordinasi dengan kementerian terkait serta melakukan evaluasi internal terhadap sistem keamanan aplikasi. Namun demikian, klarifikasi tersebut tidak mengakhiri persoalan normatif, karena UU PDP memandang kegagalan pelindungan data tidak semata-mata dari terbuktinya peretasan secara teknis, melainkan dari terganggunya jaminan keamanan, kerahasiaan, dan kepercayaan publik terhadap pengelolaan data pribadi.

Berdasarkan uraian fakta normatif tersebut, perlu ditentukan terlebih dahulu kedudukan hukum PT Pertamina (Persero) dalam kerangka UU PDP guna menilai relevansi kewajiban dan pertanggungjawaban yang melekat dalam pemrosesan data pribadi melalui aplikasi MyPertamina.

2. Kedudukan PT Pertamina (Persero) sebagai Pengendali Data Pribadi dalam Aplikasi MyPertamina

Data yang dilaporkan bocor mencakup data pribadi yang bersifat spesifik sebagaimana dimaksud dalam UU PDP, serta data pribadi lain yang memiliki karakteristik sensitif karena tingkat risikonya terhadap subjek data. Kebocoran data pada aplikasi MyPertamina bukan bukan semata dipandang sebagai persoalan teknis, melainkan menimbulkan persoalan normatif serius terhadap pemenuhan kewajiban dalam UU PDP, yang mencakup kategori data pribadi berupa NIK dan data terkait profil keuangan (subsidi BBM). Mengacu pada Pasal 4 UU PDP, kombinasi data ini memungkinkan identifikasi unik yang berisiko tinggi bagi subjek data. Urgensi pelindungan ini menjadi bersifat sistemik karena adanya integrasi langsung dengan basis data Ditjen Dukcapil. Ketika NIK yang bersifat wajib dan sensitif terkoneksi dengan layanan publik, tanggung jawab pengendali data (seperti PT Pertamina) bergeser menjadi tanggung jawab mutlak (strict liability). Kegagalan menjaga keamanan integrasi antarlembaga ini tidak hanya mencederai prinsip kerahasiaan dalam Pasal 3 UU PDP, tetapi juga berpotensi memicu krisis kepercayaan publik terhadap stabilitas layanan nasional dan keamanan identitas kependudukan digital di Indonesia.

Aplikasi MyPertamina dikembangkan dan dioperasikan sebagai sarana pendukung kebijakan subsidi energi nasional, dengan mengandalkan pemrosesan data pribadi pengguna secara terpusat dan berkelanjutan. Dalam konteks UU PDP, kedudukan hukum pihak yang mengelola data ditentukan bukan oleh siapa yang secara teknis mengoperasikan sistem, melainkan oleh siapa yang menentukan tujuan dan cara pemrosesan data pribadi.

Berdasarkan Pasal 1 angka 4 UU PDP, Pengendali Data Pribadi adalah setiap pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi. Dalam kasus MyPertamina, PT Pertamina (Persero) menentukan tujuan pemrosesan data yakni verifikasi identitas pengguna dan pengendalian distribusi bahan bakar minyak bersubsidi, serta menetapkan kerangka operasional penggunaan data tersebut. Oleh karena itu, secara normatif PT Pertamina (Persero) berkedudukan sebagai Pengendali Data Pribadi, terlepas dari adanya pihak ketiga yang terlibat sebagai penyedia atau pengelola teknis sistem.

Kedudukan ini diperkuat oleh Pasal 35 UU PDP yang menyatakan bahwa Pengendali Data Pribadi bertanggung jawab atas seluruh pemrosesan data pribadi yang berada dalam penguasaannya. Norma ini menegaskan bahwa tanggung jawab hukum tidak dapat dialihkan dengan alasan pelibatan vendor atau pihak lain. Dengan demikian, setiap risiko dan

konsekuensi hukum yang timbul dari pemrosesan data pribadi dalam aplikasi MyPertamina secara normatif tetap melekat pada PT Pertamina (Persero).

Pemrosesan data pribadi dalam konteks MyPertamina juga memiliki karakter khusus karena melibatkan data kependudukan yang digunakan untuk kepentingan publik. Hal ini menempatkan Pengendali Data pada posisi yang menuntut standar kehati-hatian yang lebih tinggi, baik dari sisi pengamanan data maupun dari sisi akuntabilitas ketika muncul indikasi kegagalan pelindungan data. Oleh sebab itu, pembahasan mengenai tanggung jawab Pengendali Data dalam kasus ini tidak dapat dilepaskan dari sifat data dan tujuan pemrosesan yang berdampak luas bagi masyarakat.

Setelah kedudukan PT Pertamina (Persero) sebagai Pengendali Data Pribadi ditetapkan secara normatif, pembahasan selanjutnya difokuskan pada bagaimana prinsip tanggung jawab mutlak administratif bekerja dalam kerangka UU PDP, khususnya dalam mengaitkan kewajiban normatif Pengendali Data dengan mekanisme sanksi administratif sebagaimana diatur dalam Pasal 57 UU PDP.

3. Penerapan Prinsip Tanggung Jawab Mutlak Administratif terhadap Pengendali Data dalam Kasus Kebocoran Data MyPertamina

Konstruksi tanggung jawab mutlak administratif sebagaimana dirumuskan dalam UU PDP memperoleh makna operasionalnya ketika diuji dalam peristiwa konkret kebocoran data pribadi yang terjadi setelah undang-undang tersebut berlaku. Kasus dugaan kebocoran data pengguna aplikasi MyPertamina menjadi contoh penting untuk menilai bagaimana kewajiban normatif Pengendali Data dan mekanisme sanksi administratif dalam UU PDP bekerja secara sistemik, tanpa harus bertumpu pada pembuktian kesalahan subjektif.

Sebagaimana telah diuraikan dalam pembahasan sebelumnya, PT Pertamina (Persero) secara normatif berkedudukan sebagai Pengendali Data Pribadi karena menentukan tujuan dan cara pemrosesan data pribadi pengguna aplikasi MyPertamina, termasuk pemrosesan data identitas kependudukan untuk keperluan pendistribusian bahan bakar minyak bersubsidi. Kedudukan tersebut menempatkan PT Pertamina (Persero) dalam lingkup kewajiban Pasal 20 UU PDP, yang mewajibkan Pengendali Data memiliki dasar pemrosesan data pribadi yang sah serta mengelola pemrosesan tersebut secara bertanggung jawab. Dalam konteks ini, Pasal 20 tidak serta-merta digunakan untuk menilai sah atau tidaknya dasar pemrosesan secara substantif, melainkan berfungsi sebagai norma awal yang menegaskan bahwa seluruh risiko pemrosesan data pribadi berada dalam penguasaan dan tanggung jawab Pengendali Data.

Kewajiban dasar tersebut kemudian dielaborasi secara lebih konkret melalui Pasal 35 UU PDP sebagai norma induk yang mewajibkan Pengendali Data memproses data pribadi sesuai dengan prinsip pelindungan data pribadi, termasuk prinsip keamanan dan pertanggungjawaban. Ketika muncul pemberitaan luas mengenai dugaan kebocoran data pengguna MyPertamina yang mencakup data identitas pengguna dan melibatkan jumlah pengguna dalam skala besar, maka secara normatif telah timbul pertanyaan serius mengenai terpenuhinya kewajiban keamanan dan pengendalian risiko sebagaimana dimaksud dalam Pasal 35. Dalam kerangka strict liability administratif, situasi ini tidak dipahami sebagai kesimpulan mengenai kesalahan teknis, melainkan sebagai indikasi kegagalan pemenuhan kewajiban normatif yang patut diuji oleh otoritas yang berwenang.

Konstruksi kewajiban tersebut diperkuat oleh Pasal 46 dan Pasal 47 UU PDP. Pasal 46 menegaskan kewajiban Pengendali Data untuk memberitahukan kegagalan pelindungan data

pribadi kepada subjek data dan lembaga pengawas dalam jangka waktu tertentu. Norma ini mencerminkan prinsip transparansi dan akuntabilitas, sekaligus menempatkan kegagalan pelindungan data sebagai peristiwa hukum administratif yang menuntut respons aktif dari Pengendali Data. Sementara itu, Pasal 47 menegaskan tanggung jawab struktural Pengendali Data atas seluruh pemrosesan data pribadi dalam penguasaannya, termasuk ketika pemrosesan tersebut melibatkan pihak lain atau sistem pendukung. Dengan demikian, tanggung jawab tidak terfragmentasi pada pelaku teknis, melainkan melekat secara normatif pada Pengendali Data sebagai pihak yang mengendalikan sistem dan tujuan pemrosesan.

Rangkaian kewajiban normatif tersebut menyatakan bahwa pengaturan sanksi dalam UU PDP dirancang sebagai instrumen administratif untuk mendorong kepatuhan pengendali data, dengan orientasi korektif dan preventif, tanpa mensyaratkan pembuktian kesalahan subjektif secara pidana (Saly et.al, 2023) memperoleh konsekuensi hukumnya secara tegas dalam Pasal 57 UU PDP. Pasal ini menempatkan pelanggaran terhadap Pasal 20 ayat (1), Pasal 35, Pasal 46, dan Pasal 47 sebagai dasar pengenaan sanksi administratif, tanpa mensyaratkan adanya pembuktian kesalahan subjektif. Karakter ini menunjukkan bahwa Pasal 57 merupakan manifestasi paling konkret dari prinsip tanggung jawab mutlak administratif dalam rezim pelindungan data pribadi Indonesia. Fokus penegakan hukum tidak diarahkan pada pencarian pelaku atau niat jahat, melainkan pada keberadaan kegagalan pelindungan data dan tidak terpenuhinya kewajiban normatif Pengendali Data.

Jenis sanksi administratif yang diatur dalam Pasal 57 ayat (2) mulai dari peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, hingga denda administratif, menunjukkan bahwa tujuan utama penegakan hukum administratif dalam UU PDP bersifat korektif dan preventif. Dalam konteks pengendalian data berskala besar seperti MyPertamina, sanksi administratif berupa denda yang dapat mencapai paling tinggi 2% dari pendapatan tahunan sebagaimana diatur dalam Pasal 57 ayat (3) memiliki fungsi penting untuk mendorong internalisasi risiko oleh Pengendali Data. Dengan mekanisme ini, kegagalan pelindungan data tidak lagi dipandang sebagai risiko eksternal yang netral, melainkan sebagai konsekuensi dari pengelolaan sistem yang harus dipertanggungjawabkan secara administratif.

Penerapan Pasal 57 UU PDP dalam kasus kebocoran data MyPertamina, oleh karena itu, tidak dimaksudkan untuk menyimpulkan kesalahan atau pelanggaran secara final, melainkan untuk menunjukkan bagaimana kerangka strict liability administratif bekerja secara normatif. Keberadaan kegagalan pelindungan data yang dipersoalkan di ruang publik, dikaitkan dengan kedudukan PT Pertamina (Persero) sebagai Pengendali Data dan sifat data yang diproses, telah cukup untuk mengaktifkan mekanisme evaluasi kepatuhan dan potensi sanksi administratif. Dengan demikian, kasus ini memperlihatkan bahwa UU PDP telah menyediakan instrumen hukum yang memungkinkan negara menegakkan pelindungan data pribadi secara efektif, tanpa terjebak pada keterbatasan paradigma pembuktian kesalahan subjektif.

Melalui analisis ini, dapat ditegaskan bahwa prinsip tanggung jawab mutlak administratif dalam UU PDP bukan sekadar konstruksi teoretis, melainkan kerangka normatif yang siap diterapkan dalam kasus konkret kebocoran data pribadi. Penerapannya terhadap kasus MyPertamina sekaligus menunjukkan urgensi konsistensi penegakan sanksi administratif sebagai bagian dari upaya menjaga kepercayaan publik dan melindungi hak subjek data dalam ekosistem digital nasional.

KESIMPULAN

Prinsip tanggung jawab mutlak (strict liability) dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan konstruksi pertanggungjawaban administratif yang berfungsi sebagai instrumen pelindungan hukum data pribadi. Prinsip ini dibangun atas pendekatan pengendalian risiko dan pemenuhan kewajiban normatif oleh Pengendali Data, bukan atas pembuktian kesalahan subjektif sebagaimana dikenal dalam hukum pidana maupun pertanggungjawaban perdata berdasarkan perbuatan melawan hukum. Dengan demikian, strict liability dalam UU PDP menempatkan hukum administrasi sebagai sarana preventif dan korektif untuk menjamin keamanan, akuntabilitas, dan kepatuhan dalam pemrosesan data pribadi, sebagaimana tercermin dalam asas pelindungan, kehati-hatian, dan pertanggungjawaban dalam Pasal 3 UU PDP. Konstruksi tanggung jawab mutlak administratif tersebut dapat digunakan secara normatif dalam menganalisis dugaan kebocoran data pada aplikasi MyPertamina, tanpa bermaksud menyimpulkan adanya kesalahan atau pelanggaran secara final. Kedudukan PT Pertamina (Persero) sebagai Pengendali Data menempatkannya dalam lingkup kewajiban Pasal 20, Pasal 35, Pasal 46, dan Pasal 47 UU PDP, yang secara sistemik bermuara pada mekanisme sanksi administratif dalam Pasal 57. Dalam konteks ini, kasus MyPertamina berfungsi sebagai ilustrasi normatif untuk menunjukkan bahwa kegagalan pelindungan data dipahami sebagai kegagalan pemenuhan kewajiban administratif, sehingga prinsip strict liability berperan sebagai dasar konseptual pelindungan hukum data pribadi dalam rezim hukum administrasi, bukan sebagai instrumen penghakiman atau penetapan tanggung jawab individual. Diperlukan penegasan konseptual yang konsisten dalam pengembangan hukum pelindungan data pribadi agar prinsip tanggung jawab mutlak administratif tidak disamakan dengan rezim pertanggungjawaban pidana maupun perdata. Penempatan strict liability secara tegas dalam ranah hukum administrasi penting untuk menjaga batas metodologis antara mekanisme kepatuhan administratif dan rezim pembuktian kesalahan, sekaligus memperkuat fungsi pelindungan hukum data pribadi yang berorientasi pada pencegahan dan pengendalian risiko. Diperlukan penyempurnaan kerangka kelembagaan dan pengaturan pelaksana terkait tata cara pengenaan sanksi administratif sebagaimana diamanatkan dalam Pasal 57 ayat (4) dan ayat (5) UU PDP. Kejelasan mekanisme tersebut diperlukan agar penerapan tanggung jawab mutlak administratif berjalan secara terstruktur dan memberikan kepastian hukum, khususnya dalam menghadapi peristiwa kebocoran data pribadi berskala besar yang melibatkan pengendali data dengan fungsi strategis dalam penyelenggaraan layanan publik.

REFERENSI

Afifah, N. (2024). Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022. Jurnal Legalitas, 2(1), 29–38.

Alatas, H. H. R. A., & Djajaputra, G. (2026). Examining Indonesian Government Accountability And Mitigation Measures In The 2024 Taxpayer Identification Number Data Breach. JIHK, 7(2), 1234–1248.

Baldwin, R., Cave, M., & Lodge, M. (2011). Understanding regulation: theory, strategy, and practice. Oxford university press.

CNN, I. (2022). Hacker Bjorka bocorkan 44 juta data MyPertamina. CNN Indonesia.

Detik.com. (2022). Bjorka klaim bocorkan data MyPertamina. Detik.Com.

Diah, & Wiraguna. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882, 2(2), 1089–1096.

Dresch, R. de F. V., & Júnior, J. L. de M. F. (2024). Special strict civil liability in Brazil's General Data Protection Law. Brazilian Journal of Law, Technology and Innovation, 2(2), 98–128.

Gizmologi.id. (2022). jorka Kembali Berulah Kini Bocorkan 44 Juta Data Pengguna MyPertamina. Gizmologi.Id.

Hadjon, P. M. (2011). Perlindungan hukum bagi rakyat di Indonesia: sebauh studi tentang Prinsip-prinsipnya... Bina Ilmu.

Hasan, F. (2024). Liability of Business Actors for the Protection of Consumer Personal Data. Mulawarman Law Review, 9(1), 12–28.

Kompas.com. (2022). Bjorka bocorkan 44 juta data MyPertamina. Kompas.Com.

Kurdi, K., & Cahyono, J. (2024). Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. JUNCTO: Jurnal Ilmiah Hukum, 6(2), 330–339.

Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. Jurnal Esensi Hukum, 5(2), 115–131.

Marzuki, P. M. (2017). Penelitian Hukum (Edisi Revisi). Kencana Prenada Media Group.

Muhaimin. (2020). Metode Penelitian Hukum. Mataram University Press.

Rofiq, A., & Pujiyono, P. (2022). Strict Liability as a Counterbalance to the Principle of Error in Indonesian Criminal Law. Journal of Judicial Review, 24(2), 319–332.

Rumbruren, A., & Watofa, Y. (2025). Analysis Of The Responsibilities Of The Organizer Of The Electronic System In Case Of Data Breach. Awang Long Law Review, 7(2), 481–491.

Rusyda, N. K. (2025). Perlindungan Hukum terhadap Subjek Data Kebocoran Data oleh Badan Publik Menurut UU Nomor 27 Tahun 2022. Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan, 2(3 SE-Articles), 247–262. https://doi.org/10.62383/desentralisasi.v2i3.940

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.

Simanjuntak, P. H. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). Jurnal Esensi Hukum, 6(2), 105–124.

Soekanto, S., & Mamudji, S. (2018). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Raja Grafindo Persada.

Wilantara, M., Renggong, R., & Zubaidah, S. (2024). Pertanggungjawaban Pelaku Tindak Pidana Peretasan Akun Pribadi Di Kota Makassar. Clavia, 22(3), 438–447.

Wiraguna, S. A., Sulaiman, A., & Barthos, M. (2024). Implementation of Consumer Personal Data Protection in Ecommerce from the Perspective of Law No. 27 of 2022. Journal of World Science, 3(3), 410–418.