

## PERTANGGUNGJAWABAN DALAM PERSPEKTIF UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI STUDI KASUS: WIFI XL AXIATA

Nursyahfitri<sup>1</sup>, Bud Abdullah<sup>2</sup>, Deva Anggraini<sup>3</sup>, Tarisa Mufidah<sup>4</sup>,  
Sastia Putri Br. Ginting<sup>5</sup>, Sاهدilang Juanda Nasution<sup>6</sup>

[nursyahfitri@insan.ac.id](mailto:nursyahfitri@insan.ac.id)<sup>1</sup>, [budiabdullah@insan.ac.id](mailto:budiabdullah@insan.ac.id)<sup>2</sup>, [devaanggarini.mhs@insan.ac.id](mailto:devaanggarini.mhs@insan.ac.id)<sup>3</sup>,  
[tarisamufidah@insan.ac.id](mailto:tarisamufidah@insan.ac.id)<sup>4</sup>, [sastiaputribrginting.mhs@insan.ac.id](mailto:sastiaputribrginting.mhs@insan.ac.id)<sup>5</sup>,  
[sاهدilangnasution.mhs@insan.ac.id](mailto:sاهدilangnasution.mhs@insan.ac.id)<sup>6</sup>

Institut Syekh Abdul Halim Hasan Binjai

**Abstrak:** Perkembangan teknologi informasi telah membawa dampak besar terhadap sistem pengelolaan data pribadi. Di Indonesia, lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi langkah krusial dalam menjamin hak privasi individu sebagai bagian dari hak asasi manusia. Penelitian ini bertujuan untuk mengkaji bentuk pertanggungjawaban hukum atas pelanggaran data pribadi berdasarkan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Metode yang digunakan adalah yuridis normatif dengan pendekatan peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa pelanggaran terhadap data pribadi dapat dikenakan sanksi dalam dua bentuk, yaitu administratif dan pidana. Sanksi tersebut diberikan kepada pengendali data maupun pihak yang terbukti melanggar ketentuan, baik karena kelalaian maupun tindakan yang disengaja. Meski secara normatif telah diatur, pelaksanaan di lapangan masih menghadapi sejumlah tantangan, seperti lemahnya pengawasan, kurangnya literasi hukum masyarakat, dan ketidaksiapan infrastruktur digital. Dengan demikian, diperlukan penguatan kelembagaan pengawas, edukasi publik yang berkelanjutan, serta mekanisme penegakan hukum yang lebih responsif. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan regulasi dan praktik perlindungan data pribadi di Indonesia.

**Kata Kunci:** Pelindungan Data Pribadi, Pertanggungjawaban Hukum, Sanksi.

**Abstract:** The development of information technology has had a major impact on the personal data management system. In Indonesia, the enactment of Law Number 27 of 2022 concerning Personal Data Protection is a crucial step in guaranteeing individual privacy rights as part of human rights. This study aims to examine the form of legal accountability for personal data violations based on the provisions of the Law Number 27 of 2022. The method used is normative juridical with a statutory regulatory approach. The results of the study show that violations of personal data can be subject to sanctions in two forms, namely administrative and criminal. These sanctions are given to data controllers and parties proven to have violated the provisions, either due to negligence or deliberate actions. Although it has been regulated normatively, implementation in the field still faces a number of challenges, such as weak supervision, lack of legal literacy in the community, and unpreparedness of digital infrastructure. Thus, it is necessary to strengthen supervisory institutions, ongoing public education, and more responsive law enforcement mechanisms. This research is expected to contribute to the development of regulations and practices for personal data protection in Indonesia.

**Keywords:** Personal Data Protection, Legal Accountability, Sanctions.

## PENDAHULUAN

Kemajuan pesat di bidang teknologi informasi dan komunikasi (TIK) mendorong pertumbuhan signifikan tidak hanya di Indonesia, tetapi juga secara global. Perkembangan ini mencakup berbagai aktivitas yang kini banyak dilakukan secara daring, mulai dari transaksi ekonomi, komunikasi, kegiatan komersial, hingga pengelolaan administrasi pemerintahan (Mahameru et al., 2023).

Dalam era transformasi digital ini, data pribadi seperti nama, alamat email, dan nomor telepon genggam memiliki nilai ekonomi yang tinggi dan menjadi komoditas penting dalam dunia bisnis. Informasi tersebut tergabung dalam apa yang disebut sebagai digital dossier atau berkas digital sebuah kumpulan data pribadi yang biasanya dimiliki oleh setiap pengguna internet. Berkas ini umumnya dikumpulkan dan dikelola oleh pihak swasta, yang kemudian menimbulkan risiko besar terhadap pelanggaran hak privasi individu (Priscyllia. 2019).

Ketertarikan yang meningkat pada teknologi komputer dan sistem digital memang membawa banyak keuntungan dalam berbagai aspek kehidupan. Namun, bersamaan dengan manfaat itu, muncul pula ancaman serius terhadap keamanan data, khususnya terkait identitas pribadi. Informasi yang awalnya bersifat privat kini lebih rentan terhadap pelanggaran, peretasan, hingga penyalahgunaan yang dapat berujung pada tindak kejahatan seperti pencurian identitas dan penipuan. Menanggapi tantangan tersebut, pemerintah Indonesia mengambil langkah strategis dengan menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Aturan ini bertujuan untuk menjaga kepercayaan publik terhadap pengelolaan informasi pribadi mereka. Selain menetapkan regulasi, pemerintah juga dituntut untuk berperan aktif dalam memastikan keamanan data dan melindungi identitas warga negara dari berbagai ancaman digital.

Informasi pribadi memiliki nilai yang sangat krusial dan perlu mendapatkan perlindungan serta pengawasan yang ketat, karena dapat dimanfaatkan secara tidak sah oleh pihak-pihak dengan maksud jahat. Perkembangan teknologi yang berlangsung dengan sangat cepat dan dinamis memunculkan kekhawatiran terhadap potensi ancaman terhadap data pribadi yang bersifat rahasia. Kondisi ini dapat membuka celah bagi terjadinya berbagai bentuk kejahatan digital, yang dikenal dengan istilah kejahatan siber. Ancaman terhadap kerahasiaan data pribadi biasanya muncul saat individu mengakses layanan digital, seperti media sosial Facebook, Instagram, Twitter, dan platform serupa yang umumnya meminta data pribadi sebagai syarat untuk membuat akun dan menikmati fitur-fiturnya. Dalam konteks ini, perlindungan terhadap informasi yang bersifat pribadi menjadi sangat vital, mengingat adanya risiko sistem yang mengalami gangguan atau kebocoran data, yang pada akhirnya dapat menimbulkan kerugian hingga tindakan melanggar hukum. Sering kali, data pribadi disalahgunakan tanpa sepengetahuan pemiliknya. Tindakan tersebut bukan hanya merugikan secara materiil maupun immateriil, tetapi juga berpotensi mencoreng reputasi individu yang datanya disalahgunakan (Gustina et al., 2022).

Di era digital saat ini, upaya perlindungan terhadap data pribadi menjadi sangat krusial untuk diterapkan. Pemerintah memiliki peran strategis dalam menjamin keamanan data tersebut melalui regulasi khusus, yakni Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan kebijakan hukum terbaru yang mengatur tata cara pengelolaan serta perlindungan data pribadi di Indonesia. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting dalam menjamin hak privasi setiap individu, khususnya terkait proses pengumpulan, pemanfaatan, serta distribusi data pribadi. Aturan ini juga memuat batasan-batasan jelas mengenai bagaimana data harus diproses dan dijaga, termasuk aspek pencatatan, persetujuan, aksesibilitas, sistem keamanan, pencegahan penyalahgunaan, sanksi hukum, hingga peran lembaga pengawas. Meski regulasi ini telah resmi diberlakukan, pemahaman masyarakat dan berbagai entitas, baik individu maupun institusi, terhadap ketentuan dan langkah-langkah preventif yang perlu diambil dalam rangka menjaga keamanan data

pribadi, masih tergolong rendah. Hal ini menunjukkan pentingnya peningkatan literasi dan kesadaran akan pentingnya perlindungan informasi pribadi di tengah arus digitalisasi yang terus berkembang (Mariani, 2020).

Artikel ini akan memusatkan perhatian pada analisis aspek hukum terkait pelanggaran data pribadi, yang dirumuskan dalam pertanyaan utama: bagaimana bentuk pertanggungjawaban hukum yang dapat diterapkan terhadap pelanggaran data pribadi berdasarkan ketentuan yang diatur dalam Undang-Undang Perlindungan Data Pribadi di Indonesia? Selain itu, akan dikaji pula jenis-jenis sanksi yang dapat dikenakan kepada pelanggar, baik berupa sanksi administratif maupun pidana. Untuk menjawab pertanyaan tersebut secara komprehensif, diperlukan kajian mendalam terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta peraturan perundang-undangan lain yang memiliki keterkaitan dengan isu perlindungan informasi pribadi di Indonesia. Pendekatan ini bertujuan untuk memperoleh pemahaman yang menyeluruh mengenai sistem perlindungan data masyarakat di era digital, serta merumuskan konsep penanganan yang tepat terhadap berbagai bentuk pelanggaran dan kejahatan yang berkaitan dengan penyalahgunaan data pribadi di masa mendatang.

## **METODE PENELITIAN**

Penelitian ini menggunakan metode yuridis normatif yang dikombinasikan dengan pendekatan empiris. Metode yuridis normatif digunakan untuk menganalisis berbagai regulasi yang mengacu pada peraturan perundang-undangan dan studi kasus terkait perlindungan data pribadi dan dokumen hukum yang relevan, sementara pendekatan empiris digunakan untuk mengumpulkan dan menganalisis data dari lapangan. Data yang digunakan dalam penelitian ini meliputi data sekunder dari literatur hukum (Wiraguna, 2024). Metode ini bertujuan untuk mengeksplorasi teori-teori hukum tentang perlindungan data pribadi dan bagaimana teori-teori ini dapat diterapkan dalam kasus tertentu. Penelitian ini juga mengkaji jenis tanggung jawab hukum yang dapat dikenakan pada individu atau perusahaan yang terbukti melanggar Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Manfaat dari penggunaan metode ini adalah memberikan pemahaman yang jelas secara teori dan norma tentang perlindungan hukum untuk data pribadi, serta memberikan dasar yang kuat dalam merumuskan saran kebijakan, memperkuat peraturan, dan praktik penegakan hukum di Indonesia.

## **HASIL DAN PEMBAHASAN**

### **Pertanggungjawaban Hukum Terhadap Pelanggaran Data Pribadi Dalam Bentuk Sanksi Pidana**

Pertanggungjawaban pidana berarti bahwa setiap individu yang melakukan kejahatan atau pelanggaran yang dijelaskan dalam hukum harus menanggung konsekuensi dari tindakan tersebut sesuai dengan kesalahannya. Dengan kata lain, individu yang terlibat dalam kriminalitas harus dihadapkan pada sanksi jika terbukti bersalah. Seseorang dinyatakan bersalah jika saat melakukan tindakan, menurut pandangan masyarakat, mencerminkan pandangan norma tentang kesalahan yang diperbuat oleh individu tersebut (Primanta, 2020). Mengacu pada Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, setiap individu yang dengan sengaja dan ilegal memperoleh atau mengumpulkan data pribadi milik orang lain dapat dikenakan hukuman penjara hingga lima tahun dan/atau denda maksimum sebesar Rp 5 miliar. Sementara itu, individu yang dengan sengaja dan tanpa izin mengungkapkan data pribadi yang bukan miliknya dapat menghadapi hukuman penjara hingga empat tahun dan/atau denda maksimal Rp 4 miliar.

Bagi individu yang dengan sengaja dan melanggar hukum menggunakan data pribadi milik orang lain, hukuman penjara yang diterapkan dapat mencapai lima tahun dan/atau denda maksimum Rp 5 miliar. Selain itu, sanksi juga berlaku bagi mereka yang dengan sengaja memalsukan data pribadi demi keuntungan pribadi atau orang lain yang dapat mendatangkan kerugian bagi pihak lain. Pelanggar yang melakukan tindakan tersebut dapat dipenjara hingga enam tahun dan/atau denda paling tinggi Rp 6 miliar. Selain mendapat sanksi pidana ini, pelaku juga mungkin akan dikenakan hukuman tambahan yang berupa pengambilan keuntungan dan/atau aset yang diperoleh dari tindakan ilegal serta pembayaran kompensasi. Apabila tindakan ini dilakukan oleh suatu perusahaan, maka sanksi dapat dikenakan kepada manajer, pemegang kontrol, pihak yang memberi instruksi, pemilik manfaat, dan/atau perusahaan tersebut. Sanksi yang bisa diterima oleh perusahaan hanya berupa denda, yang jumlahnya tidak boleh lebih dari sepuluh kali lipat dari denda maksimum yang terancam (Harruma. I. 2022). Ada empat kesalahan yang bisa mendapat hukuman pidana menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi:

- 1) Mengungkapkan informasi pribadi milik orang lain atau doxing. Tindakannya dapat berujung pada hukuman penjara dengan maksimal empat tahun dan denda hingga Rp4 miliar.
- 2) Mengumpulkan informasi pribadi dengan cara yang tidak sah. Pelanggar dapat dijatuhi hukuman penjara maksimum lima tahun dan denda maksimal Rp5 miliar.
- 3) Memanfaatkan informasi pribadi orang lain. Salah satu contoh tindakan ini adalah mendaftar kartu SIM dengan menggunakan identitas orang lain. Pelakunya menghadapi ancaman penjara maksimal lima tahun dan denda hingga Rp5 miliar.

Membuat informasi pribadi yang tidak valid atau memalsukan data pribadi. Pelakunya akan dihukum penjara dengan maksimal enam tahun dan denda sebesar Rp6 miliar.

### **Pertanggungjawaban Hukum Terhadap Pelanggaran Data Pribadi Dalam Bentuk Sanksi Administratif**

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menerapkan hukuman administratif sebagai bentuk peringatan dan saran terhadap pengolahan data pribadi yang tidak memiliki dasar yang jelas. Hukuman ini juga diterapkan untuk pelanggaran yang berkaitan dengan kesesuaian tujuan pengolahan data pribadi, serta pelanggaran dalam mendapatkan izin dari subjek data pribadi.

Sanksi yang bersifat administratif dapat mencakup teguran tertulis, penghentian sementara pengolahan data pribadi, penghapusan atau pemusnahan data pribadi, serta denda administratif yang dapat mencapai 2% dari pendapatan atau penerimaan tahunan. sesuai dengan jenis pelanggaran yang dilakukan (Putri. I. A. 2023).

Sanksi administratif terkait pelanggaran data pribadi telah diatur secara jelas di dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi serta peraturan yang menyertainya. Jenis-jenis sanksi administratif ini mencakup:

- 1) Pemberian peringatan, baik lisan maupun tulisan, kepada pengelola data pribadi yang telah melakukan pelanggaran.
- 2) Penangguhan sementara dari kegiatan pengolahan data pribadi yang tidak sesuai dengan aturan yang ditetapkan.
- 3) Penghapusan atau pemusnahan data pribadi yang telah diproses secara ilegal.
- 4) Denda administratif yang dapat mencapai maksimum 2% dari pendapatan tahunan pengelola data pribadi terkait variabel pelanggaran yang dilakukan.

Sanksi administratif ini dimaksudkan untuk menciptakan efek jera serta memastikan bahwa pengelola data pribadi melaksanakan tanggung jawabnya dengan penuh kehati

hatian dan keseriusan dalam mengelola data pribadi. Sanksi administratif menjalankan dua fungsi penting, yaitu mencegah dan menghukum. Fungsi mencegah berusaha untuk mendorong pengendali data agar mengikuti aturan perlindungan data pribadi dari awal, sedangkan fungsi menghukum bertujuan untuk memberikan efek jera agar pelanggaran tidak terjadi lagi. Dengan penerapan sanksi administratif ini, diharapkan pengelolaan data pribadi dapat berjalan dengan lebih aman dan dapat dipercaya, sehingga masyarakat merasa terlindungi dalam setiap kegiatan digital mereka.

Sesuai dengan Pasal 40A UU ITE, pemerintah memiliki tugas untuk membuat ekosistem digital yang adil, bertanggung jawab, aman, dan kreatif. Ini berarti bahwa pemerintah juga harus bertanggung jawab untuk mengelola Data Pribadi. Namun, sampai saat ini, aturan mengenai sanksi administratif untuk pemerintah masih belum ada. sementara sanksi tersebut hanya berlaku untuk pihak swasta. Oleh karena itu, perlu ada aturan yang segera dibuat bagi pemerintah untuk menciptakan dan menjaga ekosistem digital sesuai dengan amanat Pasal 40A UU ITE.

Ketidakmampuan untuk menjaga data pribadi sesuai dengan ketentuan Pasal 46 ayat (1) dan (3) serta Pasal 47 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi akan berujung pada sanksi administratif. sesuai dengan ketentuan yang terdapat dalam Pasal 40A ayat (5) UU ITE. Sanksi ini dapat berupa:

1. Peringatan atau surat teguran
2. Denda administratif
3. Penghentian sementara dari kegiatan pemrosesan data pribadi
4. Penghapusan atau pemusnahan data pribadi
5. Pemutusan akses

Jadi sudah jelas tentang kewajiban pemerintah untuk memenuhi salah satu hak warganya yaitu hak privasi dengan melindungi data pribadi masyarakat, terutama di Indonesia. Tetapi jika pemerintah gagal dalam melaksanakan hal tersebut, hukuman yang diberikan dalam konteks tanggung jawab jabatan pemerintah untuk kegagalan melindungi data pribadi bisa berupa hukuman administratif atau hukuman perdata. Dari sudut pandang tanggung jawab pribadi, hukuman bisa berupa hukuman administratif, hukuman perdata, atau hukuman pidana.

### **Perlindungan Hukum Konsumen Atas Data Pribadi**

Presiden Jokowi menandatangani Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi pada 17 Oktober 2022. Undang-undang ini bertujuan untuk melindungi data pribadi masyarakat yang dikelola oleh penyelenggara elektronik atau PSE dan mencegah orang yang tidak bertanggung jawab menyalahgunakannya. Sementara kemajuan teknologi dan internet terus berkembang dan selalu ada kejahatan di dalamnya, masalah kebocoran data harus menjadi perhatian utama dan solusi yang pasti dan aman harus diberikan segera. Kejahatan siber pasti berdampak pada individu, kelompok, dan negara. Selain itu, kerugian tersebut mencakup kerugian dalam bidang ekonomi, perbankan, politik, atau bahkan keamanan nasional.

Setelah disahkan, undang-undang perlindungan data pribadi ini diharapkan akan menjadi titik terang untuk kebocoran data pribadi yang sering terjadi di Indonesia. Menurut Naskah Akademik Undang-Undang Perlindungan Data Pribadi, "hak privasi melalui perlindungan data pribadi merupakan elemen 49 kunci bagi kebebasan dan harga diri individu." Oleh karena itu, tujuan pembentukan undang-undang perlindungan data pribadi adalah untuk melindungi kepentingan konsumen dari penyalahgunaan data pribadi mereka.

RUU Perlindungan Data Pribadi sangat urgen untuk segera disahkan mengingat masa sekarang ini teknologi sudah semakin canggih dan dalam masa pandemi. Contohnya

adalah penggunaan platform e-commerce. RUU Perlindungan Data Pribadi termasuk sangat penting dalam menjamin hak warga. Hingga pada 2020, RUU Perlindungan Data Pribadi telah ditandatangani oleh Presiden Joko Widodo.

Berdasarkan Pasal 3 RUU Perlindungan Data Pribadi, RUU Perlindungan Data Pribadi mengutamakan privasi dan mengimbangi tanggung jawab antara pemilik data dan pengendali data. Data pribadi terdiri dari dua kategori: data pribadi umum dan data pribadi spesifik. Selain itu, RUU Perlindungan Data Pribadi memberikan ketentuan yang lebih jelas tentang larangan yang terkait dengan penggunaan data pribadi. RUU Perlindungan Data Pribadi akan mengenakan sanksi administratif dan pidana untuk mencegah dan menghukum pencurian data.

#### **Contoh Kasus: Wifi XL Axiata**

Berdasarkan wawancara langsung dengan korban, Ibu Fazmi Ayu Anjani di peroleh informasi bagaimana kasus bocornya data pribadi beliau menyampaikan :

Saya menduga bahwa data pribadi yang bocor meliputi nama lengkap, nomor telepon, dan alamat rumah lengkap. Hal ini terbukti dari fakta bahwa seseorang yang bukan staf resmi XL Axiata mengetahui dan mendatangi alamat saya dengan mengatasnamakan pihak XL.

Secara non-materiil, saya mengalami rasa tidak aman dan khawatir terhadap keselamatan pribadi karena orang asing mengetahui lokasi tempat tinggal saya. Saya juga merasa trauma dan cemas terhadap potensi penipuan atau tindak kejahatan di masa depan. Secara materiil, sejauh ini belum ada kerugian finansial, tetapi saya khawatir data saya bisa disalahgunakan untuk phishing, penipuan, atau transaksi ilegal.

Data yang bocor bukan termasuk data spesifik seperti biometrik atau kesehatan, namun termasuk data pribadi penting, yaitu alamat rumah dan nomor telepon, yang dapat digunakan untuk melacak identitas dan lokasi saya secara langsung, sehingga tetap menimbulkan risiko besar terhadap privasi dan keamanan pribadi.

Ya, saya telah menyampaikan keberatan dan permintaan klarifikasi kepada pihak XL Axiata mengenai kejadian ini. Pihak XL hanya memberikan permintaan maaf secara lisan melalui staf resmi, tanpa tindak lanjut atau penjelasan tertulis mengenai sumber kebocoran data maupun langkah perlindungan yang mereka ambil.

Saya telah melakukan beberapa tindakan, antara lain: Mengganti kata sandi dan PIN pada akun serta aplikasi yang terhubung dengan nomor XL saya, Tidak lagi memberikan data pribadi kepada pihak mana pun tanpa verifikasi resmi. Melaporkan kejadian tersebut kepada pihak XL Axiata secara langsung. Mencatat dan mendokumentasikan insiden sebagai bukti apabila diperlukan untuk laporan ke lembaga berwenang atau langkah hukum selanjutnya. saya mempertimbangkan untuk mengajukan gugatan perdata jika tidak ada tindak lanjut yang jelas dari pihak XL. Dasar tuntutan saya adalah kelalaian dalam menjaga keamanan data pribadi pelanggan, sebagaimana diatur dalam Pasal 39 dan Pasal 19 UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Untuk besaran ganti rugi, saya masih akan menyesuaikan berdasarkan kerugian non-materiil (rasa takut, ketidaknyamanan, dan ancaman terhadap privasi) yang saya alami, serta biaya perlindungan tambahan yang mungkin perlu saya keluarkan.

#### **KESIMPULAN**

Berdasarkan hasil analisis terhadap kasus dugaan kebocoran data pribadi yang dialami oleh pelanggan XL Axiata, dapat disimpulkan bahwa insiden ini menunjukkan lemahnya sistem perlindungan data pribadi pada sektor telekomunikasi, khususnya dalam menjaga kerahasiaan informasi pelanggan. Data yang diduga bocor meliputi nama lengkap, nomor telepon, dan alamat rumah, yang tergolong sebagai data pribadi penting

dan berpotensi digunakan untuk melacak identitas serta lokasi individu secara langsung.

Dampak yang timbul bersifat signifikan pada aspek non-materiil, yaitu munculnya rasa tidak aman, kekhawatiran terhadap keselamatan pribadi, serta trauma psikologis akibat ketidakpastian perlindungan privasi. Meskipun belum terdapat kerugian finansial secara langsung, potensi penyalahgunaan data untuk penipuan, phishing, atau aktivitas ilegal tetap menjadi ancaman nyata bagi korban.

Respons perusahaan yang terbatas pada permintaan maaf secara lisan tanpa tindak lanjut atau penjelasan tertulis menunjukkan masih rendahnya akuntabilitas dan transparansi pengendali data dalam menangani insiden kebocoran. Hal ini bertentangan dengan prinsip perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya terkait kewajiban pengendali data untuk menjamin keamanan, memberikan pemberitahuan, dan melakukan penanganan atas pelanggaran data.

Dengan demikian, kasus ini menegaskan pentingnya penguatan tata kelola perlindungan data pribadi, peningkatan transparansi dan tanggung jawab korporasi, serta pengawasan yang lebih efektif dari otoritas berwenang. Selain itu, diperlukan pula peningkatan literasi digital masyarakat agar individu lebih waspada dalam melindungi informasi pribadinya dan mampu mengambil langkah mitigasi yang tepat saat menghadapi dugaan kebocoran data.

#### **DAFTAR PUSTAKA**

- Sustain. (2024, January 16). Empat perbuatan yang dilarang dan sanksinya berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).
- Primanta, A. I. (2020). Pertanggungjawaban pidana pada penyalahgunaan data pribadi. *Jurist Diction*, 3(4), 1431.
- Putri, I. A. (2023, August 31). Pelanggar data pribadi: Antara sanksi administratif dan pidana. *Ignos Law Alliance*. Azzahra, Reynaldi Farah, dkk. 2020. "Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Perlindungan Data Pribadi". Retrieved from: <https://fh.unpad.ac.id/urgensi-perlindungan-data-> (Diakses pada tanggal 12 Mei 2024)
- Gillang Achmad Riyadi Ilmu Hukum Fakultas Hukum Universitas Islam Bandung '' Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi'' ( Diakses pada tanggal 12 Mei 2024 )