Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome

INFO PENULIS

Diah Putri Hasian
Universitas Esa Unggul
diahputrihasian4@student.esaunggul.ac.id

Annisa Fitria
Universitas Esa Unggul
annisa.fitria@esaunggul.co.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 2, Agustus 2025
https://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Hasian, D. P., & Fitria, A. (2025). Pertanggung Jawaban Telkomsel Atas Kebocoran Rahasia Data Pribadi Pengguna Indihome. *Arus Jurnal Sosial dan Humaniora, 5* (2),1812-1821.

Abstrak

Penelitian ini bertujuan untuk mengkaji tanggung jawab hukum Telkomsel atas terjadinya kebocoran data pribadi pelanggan layanan IndiHome dengan mengacu pada ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Sebagai pihak yang berperan sebagai pengendali data, Telkomsel seharusnya menjalankan prinsip data protection by design and by default. Namun, insiden kebocoran data yang terjadi pada tahun 2020 dan 2022 menunjukkan adanya kelemahan dalam sistem pengawasan internal dan kegagalan dalam pelaksanaan prinsip tersebut secara optimal. Penelitian ini menggunakan pendekatan yuridis normatif dan konseptual, dengan metode kualitatif yang berfokus pada analisis hukum positif serta studi kasus aktual mengenai pelanggaran data. Hasil dari penelitian ini ialah Telkomsel dinilai telah melanggar ketentuan Pasal 39, 46, dan 47 UU PDP, yang mewajibkan pengendali data untuk menjaga keamanan informasi, melaporkan insiden secara tepat waktu, dan memberikan kompensasi kepada korban atas dasar prinsip tanggung jawab mutlak (strict liability). Implikasi hukum dari pelanggaran ini mencakup potensi dikenakannya sanksi administratif, perdata, hingga pidana. Oleh karena itu, diperlukan penguatan sistem keamanan siber, peningkatan transparansi audit, serta pembentukan otoritas pengawas independen sebagai bentuk langkah preventif dan represif dalam mencegah terulangnya pelanggaran serupa di masa mendatang.

Kata kunci: Pe rlindungan Data Pribadi, Telkomsel, IndiHome, Kebocoran Data, Pertanggungjawaban Hukum, UU PDP.

Abstract

This research aims to examine Telkomsel's legal liability in relation to the breach of personal data belonging to customers of the IndiHome service, with reference to the provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). As a party acting as a data controller, Telkomsel is expected to implement the principle of data protection by design and by default. However, the data breach incidents that occurred in 2020 and 2022 reveal weaknesses in internal oversight systems and a failure to effectively apply these principles. This research adopts a normative and conceptual juridical approach, employing qualitative methods that focus on the analysis of positive law and actual case studies involving data violations. Based on the findings, Telkomsel is considered to have violated Articles 39, 46, and 47 of the PDP Law, which obligate data controllers to ensure data security, report incidents in a timely manner, and provide compensation to affected individuals under the principle of strict liability. The legal implications of these violations include the potential imposition of administrative, civil, and criminal sanctions. Therefore, strengthening cybersecurity governance, improving audit transparency, and establishing an independent supervisory authority are deemed necessary as both preventive and repressive measures to avoid the recurrence of similar violations in the future.

Keywords: Personal Data Protection, Telkomsel, IndiHome, Data Breach, Legal Liability, PDP Law.

A. Pendahuluan

Perkembangan teknologi digital berhasil mengubah pandangan masyarakat untuk dapat mengakses layanan komunikasi, misalnya pada layanan internet di rumah, kantor, sekolah, atau tempat layanan umum yang lain. Kemunculan era digital informasi dimulai ditemukannya internet yang kemudian diikuti dengan komputer dan ponsel pintar. M.Muhammad dalam jurnalnya mengatakan bahwa, teknologi informasi dapat diartikan sebagai salah satu bentuk perkembangan zaman yang dampaknya dapat dirasakan oleh masyarakat Indonesia yang salah satu nya adalah layanan internet (Muhammad & Nugroho, 2021).

Di Indonesia, digitalisasi berkembang pesat dengan 175 juta pengguna internet terjadi di awal tahun 2021 yang penggunaannya mencakup sektor privat maupun sektor publik (Dhianty, 2022) . Salah satu layanan internet yang pada umumnya digunakan oleh masyarakat adalah IndiHome yang penanggung jawabnya adalah Telkomsel. Telkomsel adalah pemegang tanggung jawab terbesar dalam melindungi rahasia data pribadi para penggunanya. Akan tetapi, beberapa temuan kasus kebocoran rahasia data pribadi terjadi dalam beberapa tahun terakhir yang menimbulkan pertanyaan yang serius terkait komitmen perusahaan dalam menjalankan prinsip keamanan siber dan perlindungan data rahasia penggunanya. Kebocoran data merupakan peristiwa dimana informasi sensitif, rahasia, atau personal diedarkan bisa terjadi karena kesalahan manusia dan bahkan hingga serangan siber.

Pada tahun 2020, fenomena kebocoran data pegiat media sosial Denny Siregar menjadi perhatian publik. Kebocoran data yang dia alami mencakup NIK (Nomor Induk Kependudukan), alamat, IMEI perangkat seluler yang dugaan nya berasal dari sistem internal Telkomsel. Hasil investigasi menunjukkan bahwa bocornya data tersebut dilakukan oleh oknum karyawan outsourcing GraPARI di Surabaya. Meskipun Telkomsel telah mengklaim bahwa sudah mematuhi standar keamanan seperti ISO 27001, akan tetapi peristiwa ini ini memperlihatkan lemahnya pengawasan internal dan integritas sistem.

Selain itu, pada tahun 2022, kejadian yang sama kembali terjadi, dimana adanya laporan kebocoran data riwayat pencarian sebanyak 26,7 juta pengguna IndiHome muncul di situs gelap *(dark web).* Data yang bocor meliputi riwayat pencarian, alamat IP, E-mail, nomor telepon dan juga NIK. Akan tetapi, Telkomsel kembali membantah tuduhan tersebut dan mengkalim bahwa jumlah pengguna Indihome hanya 9,2 juta. Ombudsman RI mencatat adanya sekitar 313 laporan keluhan terkait layanan Telkomsel Indonesia dari tahun 2018 hingga 2022, termasuk penundaan berlarut dan juga penyimpangan prosedur.

C.Sutrisna dalam jurnalnya menyatakan bahwa kebocoran data terparah di Indonesia adalah ketika terindikasi bocornya data kependudukan melalui data BPJS mencapai angka 279 juta data, dimana data tersebut bersifat pribadi yang sifatnya sangat sensitif apabila diakses oleh pihak lain (Sutrisna, 2021). Dari sisi regulasi, Indonesia masih tertinggal dalam menyediakan payung hukum yang komprehensif (Mayasari, 2020). Dengan dibentuknya regulasi Perlindungan Data Pribadi diharapkan mampu meningkatkan standart keamanan rahasia data pribadi dan memastikan standart keamanan yang lebih ketat meskipun Telkomsel dengan tegas

mengklaim bahwa data pelanggan telah disimpan di server yang berbeda dan melakukan mitigasi secara rutin, namun insiden yang terjadi berulang dapat menunjukkan bahwa kebijakan internal belum sepenuhnya terlaksana secara efektif.

Efek dari bocornya rahasia data tidak hanya bersifat finansial, akan tetapi juga dapat mengancam privasi dan keamanan digital pengguna. Hal ini dapat ditunjukkan bahwa data riwayat pencarian dapat digunakan untuk memetakan kebiasaan pengguna, selain itu, NIK atau identitas lain dapat digunakan untuk membuat identitas palsu. Regulasi di Indonesia saat ini belum tegas dalam menangani kebocoran data (Setiawan & Najicha, 2022). Oleh sebab itu, Pertanggungjawaban Telkomsel harus mencakup 3 point utama yaitu,transparansi investigasi, perbaikan sistem keamanan dan juga kompensasi terhadap korban. Tanpa melakukan langkah yang bijak, tingkat kepercayaan publik terhadap layanan IndiHome akan semakin mengalami penurunan.

B. Metodologi

Penelitian ini bersifat yuridis normatif Penelitian ini bersifat yuridis normatif dengan mengkaji peraturan/regulasi dan pendekatan studi kasus dengan cara mempelajari bahan dasar hukum, menelaah prinsip-prinsip hukum, teori hukum, norma, dan pendapat para ahli hukum, menggunakan pendekatan kualitatif dengan bahan hukumnya adalah

a. Bahan Hukum Primer:
    1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
    2. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)
b. Bahan Hukum Sekunder:
    1. Buku, Artikel, dan juga Jurnal Ilmiah
    2. Laporan Penelitian
    3. Situs web resmi
    4. Berita dan Opini

Penelitian ini juga menggunakan dua pendekatan utama diantaranya adalah *Statute Approach* atau Analisis peraturan perundang-undangan untuk menilai konsistensi norma hukum dan *Conseptual Approach* atau pendekatan konsep yang mengeksplorasi doktrin dalam ilmu hukum, untuk mengembangkan gagasan baru terkait perlindungan data.

C. Hasil dan Pembahasan

Pertanggungjawaban Telkomsel Berdasarkan Undang-Undang Perlindungan Data Pribadi

Tanggung jawab diartikan menurut responsibility merupakan keawjiban bertanggung jawab atas undang undang yang memberbaiki ditimbulkan. berlaku kerusakan Teori serta yang pertanggung jawaban hukum dikenal dengan istilah legal liability theory adalah teori yang menjelaskan tentang prinsip yang mengatur kewajiban seseorang atau suatu badan hukum atas kecerobohan mengakibatkan yang kerugian, pelanggaran hak atau membahayakan orang lain. Teori ini menjadi pondasi yang bertujuan untuk menentukan siapa yang harus menanggung konsekuensi putusan hukum dan bagaimana sanksi atau kompensasi diberikan. Pertanggung jawaban hukum adalah suatu kewajiban subjek hukum misalnya, perorangan, perusahaan maupun negara untuk menerima konsekuensi hukum yang disebabkan oleh pelanggaran hukum (pidana, perdata, administrasi), kegagalan memenuhi kewajiban kontrak serta menimbulkan kerugian pihak lain. Pertanggungjawaban hukum dapat dibagi menjadi beberapa jenis diantaranya:

1. Pertanggungjawaban Pidana (*Criminal Liability*)
   Pertanggungjawaban pidana merupakan kewajiban seseorang untuk menjalankan konsekuensi hukum atas pelanggaran aturan yang diatur dalam undang-undang. Malla Avilia menjelaskan bahwa pertanggungjawaban pidana dapat diartikan sebagai pertanggungjawaban seseorang terhadap perbuatan pidana yang dilakukaannya (Malla Avila, 2022).
2. Pertanggungjawaban Perdata (*Civil Liability*)
   Pertanggung jawaban Perdata dapat diartikan sebagai kewajiban individu, atau badan hukum untuk memberikan keringanan atau kompensasi yang disebabkan oleh pelanggaran hak perdata pihak lain. Widiastuti menyebutkan bahwa pertanggungjawaban ini muncul ketika kewajiban kontraktual (yang bersumber dari

hubungan perjanjian yang disepakati oleh para pihak) atau kewajiban non kontraktual (yang diatur secara eksplisit oleh Undang-Undang) tidak terpenuhi (Widiastuti, 2020). Kewajiban kontaktual merupakan kewajiban yang muncul dari hubungan kontraktual. Ini menunjukkan adanya kesengajaan hubungan yang ditetapkan dan disepakati oleh pembuat perjanjian. Sedangkan kewajiban non kontraktual adalah kewajiban yang ditentukan oleh Undang-Undang.

3. Pertanggungjawaban Administratif (*Administrative Liability*)
   Pertanggungjawaban administratif adalah kewajiban perorangan, perusahaan maupun instansi pemerintah untuk mendapat sanksi administratif yang disebabkan oleh pelanggaran terhadap aturan yang diatur oleh hukum administrasi negara.

Teori pertanggungjawaban hukum akan terus mengalami perkembangan sejalan dengan perkembangan sosial, ekonomi serta teknologi. Pada hakikatnya teori ini tidak semata tentang menghukum, akan tetapi juga bertujuan untuk menciptakan sistem yang adil, efisien, dan responsif terhadap kebutuhan masyarakat. Pemahaman akan teori ini sangat penting guna menjaga keseimbangan antara individu, kepentingan umum, serta ketetapan hukum.

Sebagai penyedia layanan telekomunikasi, Telkomsel memiliki peran strategis sebagai pengendali data pribadi, yaitu entitas yang menentukan tujuan dan sarana pemrosesan data pelanggan. Dalam menjalankan perannya, Telkomsel wajib mematuhi ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang secara eksplisit mengatur tanggung jawab pengendali data untuk memastikan bahwa setiap pemrosesan dilakukan berdasarkan dasar hukum yang sah, seperti persetujuan subjek data atau kewajiban kontraktual. Pengendali juga diwajibkan menjaga keamanan data agar terhindar dari akses ilegal, penyalahgunaan, atau kebocoran, serta wajib memberikan pemberitahuan resmi kepada pemilik data dan Kementerian Komunikasi dan Informatika (Kominfo) dalam waktu 72 jam apabila terjadi insiden kebocoran. Di samping itu, Telkomsel juga harus memberikan akses kepada subjek data untuk memperbaiki, menghapus, atau menarik kembali persetujuan atas pemrosesan data mereka, serta menunjuk pejabat perlindungan data pribadi (DPO) apabila cakupan pemrosesan tergolong masif atau melibatkan data sensitif.

Dalam konteks UU PDP, penting untuk membedakan antara data pribadi umum seperti nama, alamat, dan nomor telepon yang meskipun terlihat sederhana, dapat disalahgunakan untuk tujuan komersial atau pencurian identitas, dan data pribadi spesifik seperti data biometrik, riwayat kesehatan, atau lokasi real-time yang berisiko tinggi karenanya disalahgunakan memerlukan dan perlindungan teknis tambahan seperti enkripsi dan pembatasan akses. Undang-Undang Perlindungan Data Pribadi juga mengakui berbagai hak subjek data, termasuk hak untuk mengetahui, mengakses, memperbaiki, hingga menghapus data mereka, serta hak atas ganti rugi jika terjadi pelanggaran.

Dalam hal Telkomsel lalai melindungi data atau gagal melaporkan insiden dalam batas waktu yang ditentukan, perusahaan dapat dikenakan sanksi administratif hingga pidana, tergantung pada tingkat pelanggaran yang terjadi. Meskipun Telkomsel telah mengklaim melakukan koordinasi dengan Kominfo dalam beberapa kasus dugaan kebocoran data, kejelasan prosedural dan transparansi tanggapan masih sangat bergantung pada hasil investigasi dan audit regulator. Oleh karena itu, kepatuhan terhadap prinsip-prinsip UU PDP menjadi hal yang krusial dalam menjaga kepercayaan publik dan akuntabilitas korporasi dalam era ekonomi digital yang berbasis data

Kegagalan ini bukan sekadar pelanggaran administratif, melainkan pembiaran struktural yang bertentangan dengan spirit Pasal 39 UU PDP. Ironisnya, sertifikasi ISO 27001 yang dimiliki Telkomsel justru menjadi bukti dekoupling antara sertifikasi dan implementasi, standar keamanan tak dioperasionalkan secara rigor, terutama pada third-party risk management. Defisit audit trail, tidak ada mekanisme forensic-ready untuk melacak data exfiltration. Ketiadaan security by design, arsitektur sistem tidak mengadopsi zero-trust model.

1. Pasal 39 Undang-Undang Perlindungan Data Pribadi Pasal 39 Undang-Undang Perlindungan Data Pribadi (UU PDP) menegaskan kewajiban fundamental pengendali data. dalam hal ini PT Telkom Indonesia (Telkomsel) sebagai penyedia layanan IndiHome untuk menjamin integritas dan kerahasiaan data pengguna melalui tiga pilar kritis diantaranya, memastikan keamanan data pribadi dengan implementasi langkah teknis (*encryption at rest & in transit, intrusion detection systems*) dan *organisatoris (role based access control, data minimization principles*), mencegah akses ilegal melalui mekanisme *multi-factor authentication, real-time access log monitoring*, dan restriksi hak akses berbasis need-to-know principle, melakukan pemantauan dan evaluasi rutin berupa *quarterly security audits, vulnerability penetration*

testing, *serta patch management systems* untuk mengatasi celah keamanan. Telkomsel, sebagai salah satu penyelenggara layanan telekomunikasi terbesar di Indonesia, secara hukum dan praktik memenuhi kriteria sebagai pengendali data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Berdasarkan Pasal 1 angka 4 UU PDP, pengendali data adalah pihak yang menentukan tujuan dan kendali atas pemrosesan data pribadi. Dalam konteks ini, Telkomsel memiliki peran aktif dalam pengumpulan, penyimpanan, pemrosesan, serta pemanfaatan data pribadi pelanggan melalui berbagai layanannya, seperti registrasi kartu SIM, aplikasi MyTelkomsel, hingga sistem penagihan dan promosi berbasis data. Selain UU PDP, Telkomsel tunduk pada ketentuan lain seperti Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Pasal 40), serta ketentuan dari Badan Regulasi Telekomunikasi Indonesia (BRTI) Kementerian Komunikasi dan dan Informatika. Sebagai pengendali data, Telkomsel memiliki sejumlah kewajiban yang harus dipenuhi, antara lain memberikan informasi secara transparan kepada pelanggan mengenai jenis dan tujuan penggunaan data pribadi, memperoleh persetujuan yang sah sebelum melakukan pemrosesan, serta menjamin keamanan data melalui sistem perlindungan yang memadai. Selain itu, Telkomsel juga diwajibkan untuk melaporkan insiden pelanggaran data pribadi kepada otoritas dan pengguna dalam waktu maksimal 3x24 jam, serta menjamin hak subjek data seperti akses, koreksi, penarikan persetujuan, dan data. Penunjukan penghapusan Petugas Pelindungan Data (*Data Protection Officer*/DPO) juga menjadi mandat penting, sebagaimana diatur dalam Pasal 53 UU PDP, untuk untuk memastikan pengawasan dan kepatuhan internal. Telkomsel pun harus mendokumentasikan seluruh proses pemrosesan data dan melakukan audit berkala untuk menjamin kepatuhan hukum. Dalam praktiknya, tanggung jawab Telkomsel terhadap pelindungan data pribadi juga mencerminkan komitmen terhadap tata kelola perusahaan yang baik (*Good Corporate Governance*), serta upaya membangun kepercayaan masyarakat dalam ekosistem digital yang kian rentan terhadap pelanggaran privasi. Dengan demikian, kepatuhan Telkomsel terhadap regulasi pelindungan data pribadi bukan sekadar kewajiban yuridis, tetapi juga menjadi bagian strategis dalam menjaga keberlanjutan bisnis dan legitimasi sosial perusahaan di era ekonomi berbasis data. Peneliti dalam hal ini, menemukan sebuah kasus yang dialami oleh infulencer Denny Siregar tahun 2020 bahwa dia mengalami kebocoran NIK, alamat, dan IMEI melalui oknum outsourcing GraPARI Surabaya mengungkap kelemahan fatal dalam access control dan pengawasan vendor pihak ketiga. Telkomsel gagal menerapkan privileged access behavioral analytics mendeteksi anomali untuk akses, mekanisme whistleblowing system internal. Selain itu, kebocoran dark web (2022) eksfiltrasi 26,7 juta data riwayat pencarian, email, dan NIK membuktikan sistematis dalam kelalaian data *loss prevention* (DLP) *tools, security information and event management* (SIEM), *dark web monitoring* untuk deteksi dini kebocoran.

Implikasi Yuridis

Kegagalan memenuhi Pasal 39 menjadi dasar pertanggungjawaban primer Telkomsel melalui Pasal 47 UU PDP (Strict Liability): Korban cukup buktikan ada kebocoran dan ada kerugian tanpa perlu membuktikan Telkomsel. kelalaian Contoh kerugian yang dapat diklaim adalah biaya pemblokiran KTP di Ditjen Dukcapil, biaya pemantauan rekening bank (fraud monitoring), ganti rugi psikologis akibat doxxing, management untuk data sensitif.

2. Pasal 46 Undang-Undang Perlindungan Data Pribadi Pasal 46 Undang-Undang Perlindungan Data Pribadi (UU PDP) menetapkan kewajiban ganda yang tidak terpisahkan bagi pengendali data seperti Telkomsel dalam merespons kebocoran data. Pertama, kewajiban cepat pelaporan (breach notification) ke Badan Siber dan Sandi Negara (BSSN) dalam waktu maksimal 3×24 jam pascaterdeteksinya insiden, yang harus mencakup tiga elemen kritis: 1. skala dan jenis data yang bocor 2. potensi dampak kerugian 3. langkah mitigasi sementara sebagaimana diatur dalam Peraturan BSSN 8/2022. Kedua, kewajiban No. audit independen tahunan oleh pihak ketiga tersertifikasi (misalnya ISO 27001 Lead Auditor) yang mencakup evaluasi kepatuhan privacy by design, uji penetrasi (penetration testing), dan audit rantai pasok (*supply chain audit*).

Bentuk Pelanggaran Yang Dilakukan Oleh Telkomsel Selaku Pengendali Data

Dalam kasus kebocoran data IndiHome 2022, Telkomsel melakukan pelanggaran berlapis diantaranya, pelaporan yang cacat substantif, keterlambatan pelaporan 7 hari (melebihi batas 72 jam), minimisasi skala kebocoran (klaim resmi 9,2 juta data vs temuan dark web 26,7 juta), penyembunyian jenis data kritis seperti NIK, kegagalan audit pascainsiden 2020, tidak

melibatkan auditor independen pascakebocoran data Denny Siregar, tidak mempublikasikan temuan audit melanggar Pasal 46 ayat (4) UU PDP.

Implikasi Hukum: Sanksi Multidimensi

Pelanggaran ini memicu tiga bentuk pertanggungjawaban yaitu sanksi administratif (Pasal 67 UU PDP), denda progresif hingga 2% pendapatan tahunan (≈Rp 1,2 triliun), pembekuan sertifikasi layanan oleh Kominfo, tanggung jawab Perdata (Pasal 47 & 58), Strict liability memungkinkan korban menuntut kompensasi tanpa pembuktian kelalaian, keterlambatan pelaporan memperparah kerugian (misal: penipuan berbasis NIK),sanksi pidana (Pasal 69), direksi berisiko pidana penjara maksimal 6 tahun jika terbukti menghambat pelaporan atau memalsukan audit.

Untuk mematuhi Pasal 46, Telkomsel harus membentuk Satgas Respons Insiden (*Breach Response Team*) berakses direksi dengan target respons <24 jam, mengintegrasikan sistem early warning dengan BSSN untuk deteksi eksfiltrasi data dark web, memublikasikan laporan audit triwulanan yang mencakup temuan kerentanan dan rencana perbaikan.

Pelanggaran Telkomsel terhadap Pasal 46 UU PDP bukan sekadar kelalaian prosedural, melainkan pembiaran struktural yang emperbesar dampak kerugian masyarakat melalui keterlambatan mitigasi, mengikis fondasi kepercayaan publik dalam ekosistem digital Indonesia, menunjukkan contempt of law (penghinaan terhadap hukum) melalui praktik minimisasi fakta dan audit semu, transformasi mendasar wajib dilakukan agar sertifikasi ISO 27001 tidak sekadar lip service, tetapi menjadi operasionalisasi nyata perlindungan data.

3. Pasal 47 Undang-Undang Perlindungan Data Pribadi

Pasal 47 Undang-Undang Perlindungan Data Pribadi (UU PDP) menetapkan prinsip tanggung jawab mutlak (*strict liability*) bagi pengendali data seperti Telkomsel, di mana pertanggungjawaban hukum atas kerugian akibat kebocoran data dibebankan secara otomatis tanpa mensyaratkan pembuktian unsur kesalahan(*fault-based liability*), sehingga korban cukup membuktikan tiga elemen kunci yaitu:

1. Terjadinya kebocoran data
2. Data pribadi korban termasuk dalam kebocoran tersebut
3. Adanya kerugian materiil atau immateriil yang timbul secara langsung dari insiden tersebut sebagaimana terlihat dalam kasus kebocoran data pengguna IndiHome 2022, dimana korban penipuan berbasis NIK tidak perlu membuktikan kelalaian teknis Telkomsel, melainkan cukup menunjukkan fakta bahwa NIKnya bocor melalui platform Telkomsel dan digunakan untuk tindak pidana keuangan.

Implikasi revolusioner prinsip ini terletak pada pembalikan beban pembuktian (*shift of the burden of proof*), bukan korban yang wajib membuktikan kelalaian pengendali data, melainkan pengendali data (dalam hal ini Telkomsel) yang harus membuktikan telah melakukan semua langkah pencegahan yang memadai (*due diligence*) sesuai Pasal 39 UU PDP seperti implementasi enkripsi *end-to-end*, *access control* ketat, dan audit rutin untuk dapat terbebas dari kewajiban ganti rugi. Namun, dalam praktiknya, pembelaan semacam ini hampir mustahil dilakukan Telkomsel setelah dua insiden beruntun (2020 dan 2022) yang membuktikan pola kelalaian sistemik, sehingga Pasal 47 menjadi senjata hukum utama korban untuk menuntut kompensasi finansial (biaya pemulihan identitas, kerugian finansial akibat penipuan), pemulihan reputasi, dan perbaikan sistem melalui gugatan perdata kolektif (*class action*). Prinsip strict liability dalam Pasal 47 UU PDP merupakan terobosan hukum yang mengadopsi standar GDPR Uni Eropa (Pasal 82) dan CCPA California, tetapi berpotensi menimbulkan disinsentif bisnis jika diimplementasikan secara kaku tanpa mempertimbangkan kompleksitas infrastruktur digital. Oleh karena itu, pengadilan perlu menerapkan uji proporsionalitas (*proportionality test*)seperti mempertimbangkan jenis data yang bocor (apakah termasuk data sensitif seperti NIK atau riwayat kesehatan), skala kebocoran, dan upaya mitigasi untuk menghindari ganti rugi yang menghancurkan (*ruinous liability*) sambil tetap menjunjung keadilan korban.

4. Pasal 58 Undang-Undang Perlindungan Data Pribadi

1. Pasal 58 Undang-Undang Perlindungan Data Pribadi menetapkan tiga pilar kompensasi restoratif yang wajib dipenuhi Telkomsel atas kebocoran data pengguna IndiHome diantaranya: Restitusi Finansia, mencakup biaya riil korban seperti pemblokiran KTP (Rp 50.000–500.000), pemantauan rekening (Rp 2–5 juta), dan ganti rugi kerugian materil akibat penipuan berbasis data bocor;
2. Pemulihan Reputasi, melalui permohonan maaf terbuka, klarifikasi publik tentang skala kebocoran sebenarnya, serta penghapusan data sensitif dari *dark web.*

3. Transformasi Sistemik, berupa perbaikan infrastruktur seperti migrasi ke *zero-trust architecture*, pembangunan *Security Operations Center* (SOC) khusus, dan penerapan *blockchain-based access logging* untuk mencegah *insider threat.*
   Implementasi ini menghadapi tantangan komplek, ambang batas kerugian immateriil (seperti trauma psikologis) yang belum terukur, mekanisme verifikasi korban yang birokratis, serta penolakan industri atas biaya transformasi mencapai 5–7% pendapatan. Secara strategis, Pasal 58 berfungsi sebagai instrumen transformasi digital yang memaksa realokasi anggaran korporasi (minimal 15% anggaran TI untuk *cybersecurity)* dan pembentukan *Data Protection Impact Assessment Boar*. Kegagalan memenuhi ketiga pilar ini berpotensi mengaktifkan sanksi kumulatif berupa denda 2% pendapatan tahunan (Pasal 67 UU PDP) di atas kewajiban restitusi.

Mekanisme Pertanggungjawaban Telkomsel atas Kebocoran Data Pengguna IndiHome

Perlindungan data pribadi merupakan bagian integral dari Hak Asasi Manusia yang bersifat fundamental. Menurut Luthfi Perlindungan data pribadi merupakan salah satu bentuk dari perlindungan Hak Asasi Manusia (HAM) (Luthfi, 2022). Data pribadi merupakan informasi sensitif yang harus dijaga dari akses dan pengguna yang tidak sah. Perlindungan data pribadi merupakan langkah atau usaha untuk menjaga keamanan dan informasi pribadi pengguna. Di Indonesia, selain HAM, perlindungan data pribadi diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) yang diberlakukan sejak 17 Oktober 2024 yang juga merupakan tonggak sejarah baru dalam perlindungan data pribadi (Niffari, 2020).

Pertanggungjawaban dalam konteks hukum merupakan pilar utama yang merepresentasikan keharusan subjek hukum baik individu, badan hukum, maupun lembaga negara untuk menanggung konsekuensi hukum atas tindakan atau kelalaian yang menimbulkan kerugian bagi pihak lain. Teori pertanggungjawaban hukum (*legal liability theory*) menjadi kerangka fundamental dalam menilai apakah suatu tindakan, baik karena kesengajaan maupun kelalaian, menimbulkan akibat hukum yang menuntut adanya sanksi atau ganti rugi, baik dalam bentuk pidana, perdata, maupun administratif. Dalam ranah perlindungan data pribadi, teori ini menjadi alat analisis penting dalam mengukur sejauh mana tanggung jawab suatu entitas digital, seperti penyedia layanan internet, dalam menjamin keamanan dan kerahasiaan informasi pengguna. Tanggung jawab tersebut bukan sekadar formalitas, melainkan mencakup penerapan prinsip kehati-hatian (*due diligence*), langkah-langkah pencegahan terhadap potensi pelanggaran, serta tanggapan cepat dan proporsional jika terjadi insiden yang melibatkan pelanggaran data.

Dalam konteks hukum positif Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara tegas menetapkan bahwa pengendali data dalam hal ini Telkomsel sebagai penyedia layanan IndiHome memiliki tanggung jawab hukum atas keamanan data pribadi milik pelanggannya. Meski demikian, sejumlah kasus yang muncul, seperti kebocoran data pribadi yang dialami oleh Denny Siregar pada 2020 dan beredarnya data pribadi 26,7 juta pengguna IndiHome di situs gelap pada 2022, menunjukkan adanya kelemahan serius dalam mekanisme perlindungan yang dijalankan Telkomsel. Padahal, ketentuan Pasal 39 UU PDP secara eksplisit mengamanatkan bahwa pengendali data wajib menjamin keamanan sistem informasi yang dikelolanya, sedangkan Pasal 46 mengatur keharusan untuk menyampaikan pemberitahuan resmi kepada otoritas berwenang dan subjek data paling lambat 72 jam sejak diketahui terjadinya pelanggaran.

Tidak berhenti di situ, Pasal 47 UU PDP memperkenalkan prinsip strict liability, yaitu tanggung jawab mutlak di mana pengendali data tetap dinyatakan bertanggung jawab secara hukum meskipun tidak terbukti adanya kesengajaan atau kelalaian secara langsung. Konsep ini mempertegas bahwa Telkomsel tidak hanya wajib bertanggung jawab secara teknis, tetapi juga secara yuridis apabila gagal menjalankan fungsi pencegahan terhadap insiden kebocoran data. Konsekuensinya, Telkomsel dapat dikenakan sanksi administratif, mulai dari teguran tertulis, denda maksimal sebesar 2% dari total pendapatan tahunan, hingga pencabutan izin pengelolaan data sebagaimana diatur dalam Pasal 57 dan 58 UU PDP.

Jika dianalisis melalui pendekatan teori pertanggungjawaban hukum, maka kelalaian yang terjadi pada Telkomsel patut dikualifikasikan sebagai kelalaian sistemik, yang mencerminkan kegagalan dalam memenuhi kewajiban administratif, serta berpotensi mengarah pada tanggung jawab perdata dan pidana, tergantung pada tingkat dampak serta kerugian yang dialami oleh pemilik data. Dalam implementasinya, Telkomsel belum menunjukkan komitmen yang utuh dalam bentuk transparansi proses investigasi, pemberian kompensasi kepada korban, serta audit keamanan digital secara terbuka yang dapat memastikan bahwa kejadian serupa tidak

akan terulang. Hal tersebut jelas bertentangan dengan prinsip perlindungan data sebagai bagian dari hak asasi manusia, sebagaimana ditegaskan oleh Luthfi (2022) bahwa informasi pribadi merupakan bagian integral dari HAM yang wajib dijamin oleh negara dan entitas privat.

Oleh karena itu, mekanisme pertanggungjawaban hukum yang semestinya dijalankan oleh Telkomsel harus bersifat menyeluruh, dimulai dari pemenuhan kewajiban notifikasi publik, pembaruan sistem keamanan internal, pelaksanaan audit independen, hingga penyediaan skema kompensasi yang layak bagi para korban kebocoran data. Apabila tanggung jawab ini diabaikan, maka pelanggaran yang terjadi tidak hanya bersifat hukum, tetapi juga mencederai etika dan integritas korporasi karena telah mengkhianati kepercayaan publik terhadap penyelenggara layanan digital nasional.

Dengan mengacu pada teori pertanggungjawaban hukum dan UU PDP, mekanisme pertanggungjawaban yang harus dijalankan oleh Telkomsel atas kebocoran data pengguna IndiHome mencakup tanggung jawab pidana, perdata, dan administratif. Tindakan Telkomsel yang tidak transparan, tidak responsif, dan tidak melakukan perbaikan sistem secara menyeluruh menunjukkan bahwa kewajiban hukum sebagaimana diamanatkan oleh UU PDP belum sepenuhnya dijalankan. Oleh karena itu, diperlukan penguatan pengawasan hukum, pemberian sanksi tegas, serta penyusunan sistem kompensasi yang adil bagi korban kebocoran data.

Dalam hal ini, kehadiran negara melalui otoritas pengawas seperti Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN) menjadi sangat penting untuk memastikan adanya penegakan hukum yang adil, tegas, dan berpihak kepada hak-hak digital warga negara.

Tantangan regulasi dalam penerapan prinsip *data protection by design* and *by default* di Indonesia untuk mencegah kebocoran data pada layanan digital seperti IndiHome

Penerapan prinsip data *protection by design and by default* di Indonesia masih menghadapi berbagai tantangan, baik dari aspek regulasi, kesiapan infrastruktur, maupun kepatuhan korporasi seperti Telkomsel dalam menyediakan layanan digital seperti IndiHome. Secara teori, pertanggungjawaban hukum yang dalam konteks ini mencakup pertanggungjawaban pidana, perdata, dan administratif berfungsi sebagai mekanisme untuk mengontrol dan memastikan bahwa pengendali data seperti Telkomsel bertindak sesuai prinsip kehati-hatian dan pencegahan (*due diligence*) terhadap potensi pelanggaran data pribadi. Namun demikian, fakta empirik seperti terjadinya kebocoran data pengguna IndiHome pada tahun 2022 menunjukkan adanya kelalaian sistemik yang melampaui aspek teknis.

Prinsip data *protection by design* yang seharusnya diimplementasikan sejak tahap perancangan sistem informasi justru tidak diterapkan secara menyeluruh, yang terlihat dari tidak adanya penerapan model arsitektur *zero-trust*, lemahnya sistem monitoring internal, serta tidak efektifnya mekanisme audit keamanan siber. Selain itu, *prinsip by default* yang mengharuskan data pribadi diproses seminimal mungkin untuk tujuan tertentu juga dilanggar, karena data sensitif seperti NIK dan riwayat pencarian dapat bocor dan diperdagangkan di forum gelap. Teori pertanggungjawaban hukum dalam hal ini menuntut adanya pembuktian bahwa Telkomsel telah lalai dalam memenuhi kewajiban perlindungan sebagaimana diatur dalam Pasal 39 dan Pasal 46 UU PDP, dan bahwa kelalaian tersebut menyebabkan kerugian yang nyata bagi subjek data. Namun, implementasi dari tanggung jawab tersebut masih menghadapi kendala akibat minimnya standar operasional nasional terkait *privacy impact assessment*, rendahnya kualitas audit independen, serta keterlambatan pelaporan insiden kepada Kominfo dan BSSN.

Oleh karena itu, tantangan utama dari regulasi saat ini adalah bagaimana memastikan bahwa prinsip pelindungan data tidak hanya menjadi slogan normatif, melainkan benar-benar terintegrasi dalam sistem manajemen risiko digital perusahaan melalui kebijakan internal yang konkret, transparansi yang tinggi, dan sanksi hukum yang konsisten agar teori pertanggungjawaban hukum dapat dijalankan secara efektif sebagai instrumen preventif dan represif.

Dari uraian diatas, beberapa point yang bisa diambil adalah sebagai berikut:

1. Prinsip data protection by design menuntut keamanan sistem sejak tahap perancangan, bukan pasca insiden.
2. Telkomsel gagal mengimplementasikan *zero-trust architecture* dan audit keamanan yang transparan.
3. Pelaporan insiden kebocoran data sering terlambat dan tidak disertai dengan informasi lengkap kepada publik.

4. UU PDP menetapkan tanggung jawab ketat (*strict liability*) bagi pengendali data seperti Telkomsel.
5. Korban kebocoran data tidak dibebani pembuktian kesalahan, cukup menunjukkan kerugian dan data bocor.
6. Tidak adanya mekanisme verifikasi korban dan kompensasi yang jelas memperlemah perlindungan hak digital.
7. Perlindungan data belum sepenuhnya menjadi budaya perusahaan; masih sebatas kepatuhan administratif.

D. Kesimpulan

Berdasarkan hasil pembahasan dan analisisyang telah dilakukan, dapat disimpulkan bahwa Telkomsel, sebagai entitas pengendali data pribadi dalam penyelenggaraan layanan IndiHome, memilikitanggung jawab hukum yang sangat besar untuk menjaga keamanan, kerahasiaan, dan integritas data milik penggunanya. Namun demikian, terjadinya kebocoran datapribadi pelanggan IndiHome pada tahun 2020 dan 2022 menunjukkan bahwa Telkomsel belum sepenuhnya melaksanakan kewajiban tersebut sebagaimana diatur dalamUndang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Berdasarkan Pasal 39, 46, dan 47 UU PDP, Telkomsel berkewajiban menerapkan pengamanan data yang memadai, melakukan pelaporan atas insiden kebocoran paling lambat 3x24 jam, dan bertanggung jawab penuh melalui prinsip strict liabilityatas segala bentuk kerugian yang timbul akibat kebocoran data.

Secara substansial, kegagalan Telkomsel dalam menjalankan kewajiban ini tidak hanya menunjukkan kelalaian teknis, tetapi juga mencerminkan kegagalan etis danstruktural dalam membangun tata kelola data pribadi yang berorientasi pada perlindungan hak subjek data. Dalam kerangka hak asasi manusia, perlindungandata pribadi merupakan bagian yang tidak terpisahkan dari hak atas privasi yang dijamin konstitusi. Oleh karena itu, bentuk pertanggungjawaban yang seharusnyadibebankan kepada Telkomsel mencakup aspek pemulihan sistem, pemberian kompensasi yang proporsional, dan penguatan sistem audit sebagai bentuktransparansi serta akuntabilitas publik.

Sebagai bentuk refleksi akademik terhadap permasalahan yang dikaji, penulis menyampaikan sejumlah rekomendasi yang bersifat konstruktif dan aplikatif. Pertama, pemerintah khususnya Kementerian Komunikasi dan Informatika (Kominfo) diharapkan segera merumuskan dan mengesahkan peraturan pelaksana dari Undang-Undang Perlindungan Data Pribadi (UU PDP), yang mencakup petunjuk teknis terkait pengamanan data, mekanisme pelaporan insiden kebocoran, serta sistem sanksi dan kompensasi yang adil bagi subjek data. *Kedua*, Telkomsel perlu memperkuat infrastruktur keamanan digitalnya dengan mengadopsi prinsip data *protection by design and by default*, disertai dengan pelatihan rutin bagi seluruh sumber daya internal mengenai pentingnya perlindungan data pribadi.

Ketiga, pembentukan lembaga pengawas independen dengan kewenangan melakukan audit, penyidikan, serta penyelesaian sengketa data pribadi secara transparan dan efisien menjadi sangat krusial. Keempat, peningkatan literasi digital masyarakat perlu didorong agar pengguna layanan telekomunikasi memiliki pemahaman yang lebih baik mengenai hak-hak mereka sebagai subjek data, termasuk mekanisme pengaduan ketika terjadi pelanggaran. Kelima, perlindungan data pribadi hendaknya dijadikan sebagai prioritas nasional dalam rangka memperkuat kedaulatan digital bangsa, dan tidak semata-mata dipahami sebagai aspek teknis dalam pengelolaan sistem informasi korporasi. Dengan implementasi berbagai saran tersebut, diharapkan dapat terwujud suatu sistem perlindungan data pribadi yang komprehensif, efektif, dan berpihak pada pemenuhan hak-hak fundamental warga negara di era digital.

E. Referensi

Nugroho, S. S., Haryani, A. T., & Farkhani. (2020). Metodologi Riset Hukum. In *ase Pustaka* (Vol. 2). https://unmermadiun.ac.id/repository_jurnal_penelitian/Sigit_Sapto_Nugroho/URL Buku Ajar/Buku Metodologi Riset Hukum.pdf

Widiastuti, Y. S. M. (2020). Asas - Asas Pertanggungjawaban Perdata. *Cahaya Atma Pustaka*, 23.

Dhianty, R. (2022). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi Rama Dhianty Abad digital informasi dimulai semenjak kemunculan internet yang diikuti dengan kemunculan

personal komputer , be. *Scripta: Jurnal Kebijakan Publik Dan Hukum*, *2*(1), 186–199. http://journal.puskapkum.org/index.php/scripta%0AKebijakan

Luthfi, R. (2022). Perlindungan Data Pribadi sebagai Perwujudan Perlindungan Hak Asasi Manusia. *Jurnal Sosial Teknologi*, *2*(5), 431–436. https://doi.org/10.59188/jurnalsostech.v2i5.336

Malla Avila, D. E. (2022). *Pertanggungjawaban Pidana Anak*. *1*(8.5.2017), 2003–2005.

Mayasari, I. (2020). Kebijakan Reformasi Regulasi Melalui Implementasi Omnibus Law Di Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(1), 1. https://doi.org/10.33331/rechtsvinding.v9i1.401

Muhammad, M. O., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi. *Pamator Journal*, *14*(2), 165–174. https://doi.org/10.21107/pamator.v14i2.12472

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976–982.

Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia. Wacana Paramarta Jurnal Ilmu Hukum, 20(5) , 1–23.