Almufi Jurnal Sosial dan Humaniora (ASH)
Website: http://almufi.com/index.php/ASH
Email: almufi.ash@gmail.com

Pelindungan Hukum terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan

INFO PENULIS

Anna Stefania Peni Henakin
Universitas Esa Unggul, Jakarta
anna22stefannia@gmail.com

I Made Kantikha
Universitas Esa Unggul, Jakarta
kanthika@esaunggul.ac.id

Helvis
Universitas Esa Unggul, Jakarta
Mey. mooi@ Yahoo. Com

Horadin Saragih
Universitas Esa Unggul, Jakarta
diensarg@gmail.com

Tuti Elawati
Universitas Sains Indonesia
tutielawati69@gmail.com

INFO ARTIKEL

ISSN: 3046-8507
Vol. 2, No. 2, Juli 2025
http://almufi.com/index.php/AJSH

Saran Penulisan Referensi:

Henakin, A. S. P., Kantikha, I. M., Helvis., Saragih, H., & Tuti Elawati, T. (2025). Pelindungan Hukum terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan. *Almufi Almufi Jurnal Sosial dan Humaniora, 2* (2), 117-128.

Abstrak

Kebocoran data pribadi peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan menjadi persoalan serius yang menuntut kehadiran hukum sebagai pelindung hak-hak fundamental warga negara, khususnya hak atas privasi. Penelitian ini bertujuan untuk menganalisis akibat hukum yang timbul akibat kebocoran data pribadi peserta BPJS Ketenagakerjaan baik bagi peserta maupun institusi penyelenggara. Metode yang digunakan dalam penelitian ini adalah yuridis normatif, dengan menggunakan teori perlindungan data pribadi, teori perlindungan hak atas privasi, dan teori perlindungan hukum. Hasil penelitian menunjukkan bahwa kebocoran data pribadi peserta BPJS menimbulkan akibat hukum berupa potensi kerugian materiel dan immateriel bagi peserta, serta tanggung jawab hukum bagi BPJS Ketenagakerjaan. Perlindungan hukum terhadap peserta saat ini masih bersifat reaktif dan belum sepenuhnya mencerminkan prinsip kehati-hatian dan akuntabilitas dalam pengelolaan data pribadi. Meskipun Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya masih menghadapi berbagai kendala, terutama dalam pengawasan dan penegakan sanksi terhadap pelanggaran. Kesimpulannya, perlindungan hukum terhadap peserta BPJS Ketenagakerjaan atas kebocoran data pribadi masih belum memadai dan membutuhkan penguatan secara normatif dan institusional. Oleh karena itu, diperlukan kebijakan perlindungan data yang lebih komprehensif, penegakan hukum yang tegas, serta peningkatan transparansi dan akuntabilitas BPJS dalam mengelola data peserta.

Kata kunci: Perlindungan hukum, kebocoran data pribadi, Jaminan Sosial.

Abstract

The leakage of personal data of participants in the Social Security Administering Body for Employment (BPJS Ketenagakerjaan) has become a serious issue that demands the presence of law as a safeguard for citizens' fundamental rights, particularly the right to privacy. This research aims to analyze the legal consequences arising from the leakage of personal data of BPJS Employment participants, both for the participants and the administering institution. The research method employed is normative juridical, utilizing the theory of personal data protection, the theory of the right to privacy, and the legal protection theory. The results show that the leakage of participants' personal data leads to legal consequences, including potential material and immaterial losses for participants and legal liability for BPJS Employment. Legal protection for participants is currently reactive and does not fully reflect the principles of prudence and accountability in the management of personal data. Although Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection, its implementation still faces various challenges, particularly in supervision and enforcement of sanctions for violations. In conclusion, the legal protection for BPJS Employment participants regarding personal data breaches remains inadequate and requires normative and institutional strengthening. Therefore, a more comprehensive data protection policy, firm law enforcement, and enhanced transparency and accountability of BPJS in managing participant data are urgently needed.

Keywords: Legal protection, personal data breach, social security.

A. Pendahuluan

Badan Penyelenggara Jaminan Sosial (BPJS) Indonesia merupakan lembaga publik yang bertanggung jawab langsung kepada Presiden Republik Indonesia dan memiliki mandat besar dalam menyelenggarakan program jaminan sosial nasional. Lembaga ini dibentuk berdasarkan Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggara Jaminan Sosial, sebagai implementasi dari amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28H ayat (3) dan Pasal 34 ayat (2) yang menegaskan hak setiap warga negara atas jaminan sosial. BPJS terdiri atas dua jenis, yaitu BPJS Kesehatan dan BPJS Ketenagakerjaan, yang masing-masing memiliki cakupan dan tugas yang berbeda namun saling melengkapi dalam sistem jaminan sosial nasional.

BPJS Ketenagakerjaan secara resmi mulai menjalankan operasional penuhnya pada tanggal 1 Juli 2015, sebagai lembaga yang menggantikan fungsi dan peran dari PT Jamsostek (Persero). Lembaga ini merupakan bagian integral dari transformasi sistem jaminan sosial nasional yang ditetapkan oleh pemerintah berdasarkan Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggara Jaminan Sosial, dengan mandat utama untuk menyelenggarakan perlindungan bagi tenaga kerja Indonesia di berbagai sektor. BPJS Ketenagakerjaan bertanggung jawab dalam menyelenggarakan sejumlah program jaminan sosial ketenagakerjaan yang mencakup Jaminan Kecelakaan Kerja (JKK), Jaminan Hari Tua (JHT), Jaminan Pensiun (JP), serta Jaminan Kematian (JKM).

Keempat program tersebut dirancang secara sistematis guna memberikan perlindungan menyeluruh bagi para pekerja terhadap berbagai risiko sosial dan ekonomi, termasuk risiko kecelakaan di tempat kerja, pemutusan hubungan kerja akibat usia pensiun, kehilangan kemampuan produktif karena cacat, serta risiko meninggal dunia yang berdampak pada kesejahteraan keluarga yang ditinggalkan. Dengan adanya perlindungan ini, diharapkan pekerja memiliki rasa aman dalam menjalankan profesinya, serta kepastian terhadap keberlangsungan penghasilan dan kelangsungan hidup di masa depan.

Awalnya, keikutsertaan dalam program-program BPJS Ketenagakerjaan diwajibkan hanya untuk para pekerja formal, seperti pegawai swasta, BUMN, dan pekerja perusahaan multinasional. Namun, dalam beberapa tahun terakhir, kebijakan perluasan peserta mulai diterapkan secara progresif untuk menjangkau pekerja informal atau sektor non-upahan seperti petani, nelayan, pedagang kaki lima, dan pengemudi ojek daring yang jumlahnya jauh lebih besar. Hal ini dilakukan melalui berbagai upaya sosialisasi, kerja sama lintas sektor, serta inovasi layanan berbasis digital guna memudahkan pendaftaran dan pembayaran iuran secara mandiri.

Kebocoran data pribadi peserta BPJS yang paling mencuri perhatian publik dan menjadi

sorotan nasional terjadi pada bulan Mei 2021, saat itu publik dikejutkan oleh laporan adanya dugaan kebocoran data dalam jumlah sangat besar yang mencapai sekitar 279 juta data penduduk Indonesia. Informasi yang bocor ini diduga tidak hanya mencakup peserta aktif BPJS Kesehatan, tetapi juga data penduduk yang sudah meninggal dunia, sehingga memunculkan spekulasi bahwa basis data yang diambil berasal dari integrasi lintas instansi yang melibatkan berbagai lembaga pemerintah. Kebocoran ini pertama kali terungkap setelah akun pengguna forum daring bernama "Kotz" mengklaim menjual data tersebut di sebuah situs gelap atau dark web yang dikenal sebagai Raid Forums, lengkap dengan contoh data yang terdiri dari Nama, Nomor Induk Kependudukan (NIK), alamat, nomor telepon, email, bahkan data terkait pekerjaan dan penghasilan.

Pada bulan Maret 2023, publik kembali digemparkan oleh klaim seorang peretas yang dikenal dengan nama samaran "Bjorka", yang menyatakan bahwa dirinya berhasil memperoleh dan menyimpan sekitar 19 juta data pribadi milik peserta BPJS Ketenagakerjaan. Data tersebut disebut-sebut mencakup informasi sensitif seperti nomor induk kependudukan (NIK), nama lengkap, alamat, hingga informasi ketenagakerjaan, dan diklaim dijual melalui forum digital gelap. Klaim tersebut dengan cepat menyebar luas di media sosial dan berbagai platform berita daring, memicu kekhawatiran masyarakat akan keamanan data pribadi yang dikelola oleh lembaga-lembaga pemerintah. ada Juni 2024, masyarakat digital Indonesia kembali dihebohkan oleh isu kebocoran data peserta BPJS Ketenagakerjaan. Isu tersebut mencuat setelah akun media sosial X (sebelumnya Twitter) dengan nama pengguna @FalconFeedsio mempublikasikan bahwa data milik peserta BPJS Ketenagakerjaan telah dipasarkan kembali di forum peretasan terkenal, yakni BreachForums, sebuah platform yang sering digunakan oleh para peretas untuk memperjualbelikan data hasil pembobolan. Informasi ini memicu kekhawatiran publik karena menyangkut keamanan data pribadi jutaan pekerja Indonesia, baik yang berada di sektor formal maupun informal, mengingat pentingnya peran BPJS Ketenagakerjaan sebagai lembaga penyelenggara jaminan sosial ketenagakerjaan.

Meskipun pihak BPJS Ketenagakerjaan telah secara tegas mengeluarkan pernyataan resmi yang memastikan bahwa data peserta tetap aman dan tidak mengalami kebocoran, namun kekhawatiran masyarakat terhadap potensi penyalahgunaan data pribadi masih tetap tinggi. Hal ini disebabkan oleh maraknya kasus kebocoran data di berbagai institusi dan lembaga lain sebelumnya, yang menimbulkan rasa tidak percaya dan ketidakpastian di kalangan publik. Masyarakat merasa khawatir bahwa data sensitif seperti Nomor Induk Kependudukan (NIK), alamat, nomor telepon, hingga informasi ketenagakerjaan bisa saja jatuh ke tangan pihak yang tidak bertanggung jawab dan digunakan untuk berbagai tindak kejahatan, seperti penipuan, pencurian identitas, atau bahkan pemerasan. Selain itu, ketidakpastian tentang bagaimana data tersebut dikelola dan dilindungi secara teknis menambah kekhawatiran masyarakat. Kepercayaan terhadap sistem keamanan data yang dimiliki lembaga publik, termasuk BPJS Ketenagakerjaan, menjadi sangat penting agar masyarakat merasa aman dan terlindungi dalam menggunakan layanan publik yang berbasis data pribadi mereka. Oleh sebab itu, transparansi, komunikasi yang jelas, serta langkah-langkah penguatan keamanan siber menjadi hal yang sangat diperlukan guna mengurangi rasa cemas masyarakat dan membangun kembali kepercayaan publik terhadap pengelolaan data pribadi di Indonesia.

Insiden-insiden tersebut menegaskan betapa krusialnya perlindungan data pribadi serta penguatan keamanan sistem informasi di Indonesia. Kasus kebocoran data yang terus berulang mengungkapkan kelemahan-kelemahan dalam pengelolaan dan penjagaan data oleh berbagai institusi, baik pemerintah maupun swasta. Hal ini menjadi peringatan penting bahwa dalam era digital yang semakin maju, sistem informasi harus dibekali dengan protokol keamanan yang mutakhir dan berlapis guna mencegah akses ilegal serta penyalahgunaan data pribadi warga negara. Selain itu, insiden ini juga menuntut adanya peningkatan regulasi yang tegas dan komprehensif terkait perlindungan data, agar ada payung hukum yang kuat bagi penanganan kasus-kasus kebocoran data di masa mendatang. Kesadaran kolektif mengenai pentingnya menjaga privasi dan keamanan data menjadi semakin penting untuk membangun kepercayaan publik terhadap penggunaan teknologi informasi dalam berbagai aspek kehidupan, terutama layanan publik. Dengan demikian, upaya memperkuat aspek keamanan digital menjadi salah satu prioritas utama dalam pembangunan infrastruktur teknologi informasi di Indonesia.

Berdasarkan yang telah penulis uraikan tersebut dalam latar belakang masalah, maka penulis tertarik untuk melakukan penelitian dalam karya ilmiah ini dengan membuat judul “Perlindungan Hukum Terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara

Jaminan Sosisal Ketenagakerjaan"

Berdasarkan uraian masalah tersebut diatas, maka penulis mempokuskan penelitian ini dengan membuat rumusan masalah tentang bagaimana akibat hukum yang timbul akibat kebocoran data pribadi peserta BPJS Ketenagakerjaan baik bagi peserta maupun institusi penyelenggara?

Untuk menganalisis rumusan masalah tersebut, peneliti menggunakan beberapa teori, yaitu:

1. Teori Perlindungan Data Pribadi

Teori perlindungan data pribadi merupakan salah satu landasan penting dalam mengatur dan melindungi hak individu atas informasi pribadinya dari berbagai bentuk penyalahgunaan, termasuk kebocoran data. Secara umum, perlindungan data pribadi mengacu pada upaya hukum dan teknis yang dilakukan untuk menjaga keamanan, kerahasiaan, dan integritas data yang bersifat pribadi agar tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Teori ini lahir seiring dengan perkembangan teknologi informasi dan komunikasi yang semakin maju, sehingga memunculkan kebutuhan untuk mengatur bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan disebarkan dengan cara yang sah dan etis. Menurut Solove (2006), perlindungan data pribadi adalah bagian dari hak atas privasi yang meliputi kontrol individu terhadap informasi pribadi yang mereka miliki. Hak atas privasi sendiri telah diakui sebagai hak asasi manusia yang fundamental dalam berbagai instrumen internasional seperti Deklarasi Universal Hak Asasi Manusia Pasal 12 dan Kovenan Internasional tentang Hak Sipil dan Politik Pasal 17.

Pencetus teori perlindungan dikembangkan oleh Samuel Warren dan Louis. Mereka menekankan pentingnya hak individu untuk mengendalikan informasi pribadi mereka agar tidak disalahgunakan oleh pihak lain. Seiring waktu, teori ini berkembang dengan memasukkan aspek-aspek teknis dan hukum modern, termasuk pengaturan tentang pengumpulan dan pengolahan data elektronik, yang sangat relevan di era digital saat ini. Organisasi internasional seperti OECD dan Uni Eropa juga telah menetapkan prinsip-prinsip perlindungan data yang menjadi acuan banyak negara, termasuk Indonesia. Misalnya, General Data Protection Regulation (GDPR) di Uni Eropa menjadi standar global dalam mengatur perlindungan data pribadi dengan penekanan pada hak subjek data dan kewajiban pengendali data.

Kaitan teori perlindungan data pribadi dengan kasus kebocoran data pribadi peserta BPJS Ketenagakerjaan sangat erat. Kebocoran data merupakan pelanggaran langsung terhadap prinsip dasar perlindungan data, yang tidak hanya merugikan peserta dari sisi keamanan dan privasi, tetapi juga menimbulkan risiko sosial dan ekonomi, seperti pencurian identitas, penipuan, dan penyalahgunaan data lainnya. Dalam kasus BPJS, data pribadi yang bocor biasanya meliputi informasi sensitif seperti nomor identitas, alamat, nomor telepon, dan data kesehatan yang seharusnya dilindungi secara ketat berdasarkan prinsip-prinsip perlindungan data. Kegagalan dalam menjaga keamanan data ini menunjukkan lemahnya implementasi teori perlindungan data pribadi dalam praktik pengelolaan data di BPJS. Hal ini menuntut adanya penguatan regulasi, pengawasan, serta peningkatan kapasitas teknis lembaga untuk menerapkan protokol keamanan data yang efektif.

Selain itu, teori perlindungan data pribadi juga menegaskan bahwa perlindungan tidak hanya bersifat preventif, tetapi juga harus diikuti oleh mekanisme penegakan hukum yang tegas terhadap pelanggaran. Dalam konteks BPJS, ketika terjadi kebocoran data, lembaga ini harus bertanggung jawab secara hukum untuk memberikan kompensasi kepada peserta yang dirugikan dan melakukan tindakan perbaikan agar kejadian serupa tidak terulang. UU PDP mengatur sanksi administratif hingga pidana bagi pihak yang terbukti lalai atau menyalahgunakan data pribadi, sehingga teori perlindungan data pribadi ini berfungsi sebagai kerangka untuk menilai apakah tindakan BPJS sudah memenuhi standar perlindungan yang diwajibkan oleh hukum.

b. Teori Perlindungan Hak Atas Privasi

Teori Perlindungan Hak Atas Privasi merupakan salah satu teori penting yang menjadi dasar pengaturan hukum mengenai data pribadi. Teori ini dikembangkan secara mendalam oleh Alan F. Westin. Westin mendefinisikan privasi sebagai hak individu untuk menentukan secara mandiri bagaimana, kapan, dan sejauh mana informasi tentang dirinya dikomunikasikan kepada pihak lain. Menurut Westin, privasi tidak hanya mencakup aspek kerahasiaan data, tetapi juga terkait erat dengan otonomi pribadi dan martabat manusia. Hak atas privasi terdiri dari empat dimensi utama, yaitu privasi informasi (informational privacy), privasi fisik (physical privacy), privasi komunikasi (communication privacy), dan privasi kebebasan berprilaku (territorial privacy).

Teori ini menegaskan bahwa data pribadi merupakan bagian integral dari identitas individu. Oleh karena itu, pengelolaan data pribadi harus dilakukan secara bertanggung jawab, proporsional, dan sejalan dengan prinsip persetujuan (consent) yang sah. Dalam kerangka hukum Indonesia, pemikiran Alan F. Westin berkontribusi membentuk prinsip-prinsip perlindungan data sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, khususnya mengenai hak pemilik data untuk memperoleh informasi, hak untuk memperbaiki data, serta hak untuk mengajukan keberatan terhadap penggunaan data yang tidak sah. Ketika terjadi kebocoran data peserta BPJS Ketenagakerjaan, pelanggaran tersebut tidak hanya menimbulkan kerugian ekonomi dan administratif, tetapi juga mencederai hak konstitusional warga negara atas rasa aman dan perlindungan diri sebagaimana dijamin dalam Pasal 28G ayat (1) UUD NRI Tahun 1945.

Teori perlindungan hak atas privasi juga menjelaskan bahwa kebocoran data dapat menimbulkan chilling effect, yakni kondisi ketika individu merasa terancam, dibatasi kebebasannya, atau kehilangan kepercayaan kepada lembaga publik. Dalam konteks BPJS Ketenagakerjaan, kebocoran data sensitif seperti data identitas kependudukan, riwayat kesehatan kerja, dan informasi rekening bank berpotensi menimbulkan kerugian imaterial yang signifikan. Oleh karena itu, teori ini menjadi dasar argumentasi mengapa pengendali data (BPJS Ketenagakerjaan) memiliki tanggung jawab hukum yang bersifat preventif, kuratif, dan represif dalam menjamin keamanan data pribadi peserta. Agustina ,2019

c. Teori Perlindungan Hukum

Teori perlindungan hukum merupakan landasan penting dalam memahami bagaimana negara memberikan jaminan dan perlindungan terhadap hak-hak warga negaranya melalui perangkat hukum yang tersedia. Teori perlindungan hukum adalah bentuk pengakuan dan perlindungan yang diberikan oleh sistem hukum kepada subjek hukum, baik individu maupun badan hukum, dalam rangka menjamin kepastian, keadilan, dan kemanfaatan atas hak-haknya yang dilanggar atau terancam dilanggar. Menurut Phillipus M. Hadjon, perlindungan hukum dibagi menjadi dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif dimaksudkan untuk mencegah terjadinya pelanggaran hak, sedangkan perlindungan hukum represif dilakukan setelah terjadi pelanggaran, dengan memberikan upaya pemulihan atau ganti rugi.

Dalam konteks hukum Indonesia, perlindungan hukum memiliki dasar yang sangat kuat, baik secara konstitusional maupun dalam peraturan perundang-undangan lainnya. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu. Ketentuan ini merupakan manifestasi dari hak asasi manusia yang wajib dijamin oleh negara. Dalam praktiknya, perlindungan hukum terhadap data pribadi juga diperkuat dengan diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang secara spesifik mengatur hak-hak subjek data serta kewajiban para pengendali data untuk menjaga kerahasiaan dan integritas data pribadi.

Selain itu, perlindungan hukum juga menuntut adanya akuntabilitas dari pengelola data. Dalam hal ini, BPJS tidak cukup hanya menyatakan bahwa sistem mereka aman atau menyangkal adanya kebocoran, tetapi juga harus memberikan bukti audit keamanan informasi yang kredibel, terbuka kepada pengawasan publik, dan kooperatif dalam proses investigasi oleh lembaga berwenang seperti Kominfo dan BSSN. Perlindungan hukum yang efektif mencakup aspek preventif melalui kebijakan keamanan siber dan teknologi yang mutakhir, serta represif melalui mekanisme penegakan hukum yang cepat, tepat, dan berkeadilan. Jika tidak, maka peserta BPJS akan terus hidup dalam kekhawatiran akan penyalahgunaan data mereka, seperti pencurian identitas atau penipuan digital, yang pada akhirnya merusak kepercayaan publik terhadap institusi negara.

Dalam hal perlindungan hukum yang represif, peserta yang merasa dirugikan juga berhak mengajukan gugatan ke pengadilan berdasarkan Pasal 58 UU PDP. Ini menunjukkan bahwa teori perlindungan hukum bukan sekadar teori normatif, tetapi memiliki konsekuensi langsung terhadap praktik hukum. Negara wajib hadir dalam memastikan setiap warga negara mendapatkan perlindungan hukum yang nyata dan bukan sekadar prosedural. Hal ini penting mengingat data pribadi kini telah menjadi komoditas bernilai tinggi di era digital. Tanpa perlindungan hukum yang kuat dan efektif, data pribadi dapat menjadi sumber kerugian, baik

secara individu maupun kolektif.

B. Metodologi

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif, yaitu penelitian yang difokuskan pada pengkajian terhadap norma-norma hukum tertulis yang mengatur perlindungan data pribadi dalam konteks jaminan sosial ketenagakerjaan. Penelitian ini tidak hanya mengkaji undang-undang dan peraturan yang berlaku, tetapi juga menelaah asas-asas hukum, teori hukum, dan prinsip-prinsip perlindungan hukum yang berkaitan dengan keamanan data pribadi peserta BPJS Ketenagakerjaan.

Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menelaah regulasi yang berkaitan dengan perlindungan data pribadi dan jaminan sosial, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 24 Tahun 2011 tentang BPJS, serta peraturan pelaksana lainnya. Sementara pendekatan konseptual digunakan untuk mengkaji teori-teori hukum dan konsep perlindungan data pribadi guna membangun argumentasi akademik yang mendalam terhadap permasalahan hukum yang diteliti.

Penelitian ini menggunakan tiga jenis bahan hukum, yaitu:

a. Bahan hukum primer, yakni peraturan perundang-undangan yang relevan sepert Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggara Jaminan Sosial, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Pasal 28G dan Pasal 28H), Peraturan Pemerintah, Peraturan BPJS, dan peraturan teknis lainnya.
b. Bahan hukum sekunder, yaitu literatur hukum, jurnal ilmiah, hasil penelitian sebelumnya, serta buku-buku yang membahas perlindungan data pribadi, hukum jaminan sosial, dan keamanan siber.
c. Bahan hukum tersier, yaitu kamus hukum, ensiklopedia hukum, dan sumber-sumber referensi lain yang mendukung pemahaman istilah dan konsep.

Teknik analisis bahan hukum yang digunakan adalah analisis kualitatif, yaitu dengan cara menginterpretasikan norma-norma hukum dan teori-teori yang relevan untuk menjawab rumusan masalah. Analisis dilakukan secara sistematis untuk mengidentifikasi kesesuaian antara norma yang berlaku dengan praktik perlindungan data di BPJS Ketenagakerjaan, serta mengkaji implikasi hukumnya apabila terjadi kebocoran data pribadi peserta. Selanjutnya, hasil analisis disajikan secara deskriptif-analitis guna memberikan gambaran komprehensif mengenai efektivitas perlindungan hukum dalam kasus kebocoran data tersebut.

C. Hasil dan Pembahasan

Akibat Hukum Yang Timbul Akibat Kebocoran Data Pribadi Peserta BPJS Ketenagakerjaan Baik Bagi Peserta Maupun Institusi Penyelenggara.

1. Akibat Hukum Bagi Peserta BPJS Ketenagakerjaan

Kebocoran data pribadi yang terjadi dalam sistem BPJS Ketenagakerjaan bukan hanya mencerminkan kelalaian administratif, tetapi membawa akibat hukum serius bagi para peserta sebagai subjek data. Akibat ini bersifat multidimensi, meliputi pelanggaran hak konstitusional, ancaman terhadap keamanan pribadi peserta, hingga tidak adanya mekanisme ganti rugi yang efektif di dalam sistem hukum positif Indonesia.Akibat hukum pertama dan paling fundamental dari kebocoran data adalah pelanggaran atas hak konstitusional dan hak privasi individu. Sebagaimana diatur dalam Pasal 28G ayat (1) UUD 1945, setiap orang berhak atas perlindungan diri pribadi dan rasa aman. Hak ini bukan hak biasa, melainkan hak konstitusional yang dijamin dan tidak dapat dikurangi dalam keadaan apapun (non-derogable right). Dengan bocornya data pribadi peserta seperti nama, NIK, alamat, penghasilan, dan riwayat klaim negara, dalam hal ini BPJS Ketenagakerjaan sebagai pengendali data, telah gagal menjalankan kewajiban konstitusionalnya untuk menjamin perlindungan tersebut.

Pelanggaran ini bukan hanya bersifat moral atau etik, tetapi juga mengandung dimensi hukum publik yang menyangkut tanggung jawab negara terhadap warganya. Peserta tidak lagi memiliki kendali atas informasi pribadinya yang semestinya hanya digunakan untuk keperluan jaminan sosial. Dengan kehilangan kontrol tersebut, maka hak atas privasi yang diakui secara universal sebagai bagian dari hak asasi manusia telah direduksi secara nyata.

Kebocoran data pribadi juga menimbulkan kerugian immaterial yang signifikan bagi peserta. Berbeda dengan kerugian materiil yang bisa dihitung secara pasti, kerugian immaterial meliputi rasa takut, kecemasan, kehilangan rasa aman, dan gangguan psikologis akibat potensi penyalahgunaan data. Di era digital, kebocoran informasi membuka peluang terjadinya berbagai kejahatan berbasis teknologi seperti doxing, phishing, scamming, dan pinjaman online ilegal yang mengandalkan data bocor untuk melakukan manipulasi identitas.

Salah satu bentuk nyata dari ancaman ini adalah social engineering, yaitu teknik manipulatif yang memanfaatkan kelemahan psikologis korban untuk memperoleh informasi lebih lanjut atau mengakses sistem pribadi, sering kali berujung pada penipuan finansial. Meski dampaknya sangat nyata, sayangnya korban sering kali kesulitan membuktikan hubungan langsung antara kebocoran data dan kerugian yang mereka alami, karena tidak adanya jejak digital yang jelas atau pelaku berada di luar yurisdiksi hukum Indonesia. Akibatnya, banyak korban yang menderita secara nyata tetapi tidak mampu menempuh jalur hukum karena hambatan pembuktian. Hal ini menimbulkan kesenjangan perlindungan hukum yang mencolok: hak dilanggar, tetapi mekanisme ganti rugi tidak tersedia atau tidak efektif.

Hingga saat ini, hukum Indonesia belum memiliki mekanisme kompensasi yang efektif bagi korban kebocoran data pribadi. Meskipun UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur hak atas ganti rugi, namun peraturan pelaksanaannya, termasuk mekanisme perhitungan dan pembuktiannya, masih belum memadai. Tidak ada standar yang jelas mengenai besaran kompensasi untuk kerugian immaterial, seperti kehilangan rasa aman atau potensi kerugian di masa depan akibat penyalahgunaan data. Proses untuk menuntut ganti rugi melalui jalur perdata juga sangat memberatkan korban. Mereka harus membuktikan adanya perbuatan melawan hukum, kesalahan atau kelalaian pihak pengendali data (dalam hal ini BPJS), serta membuktikan hubungan kausal antara kebocoran data dengan kerugian yang diderita. Sementara itu, BPJS sebagai badan publik sering kali berlindung di balik argumen bahwa kebocoran disebabkan oleh serangan siber atau pihak ketiga yang tidak dapat dikendalikan.

Ketiadaan lembaga penyelesaian sengketa yang bersifat non-litigatif dan pro-korban juga memperparah situasi. Dalam konteks ini, Lembaga Pengawas Pelindungan Data Pribadi sebagaimana diamanatkan UU PDP belum terbentuk secara fungsional. Akibatnya, peserta yang menjadi korban tidak memiliki saluran remediasi yang cepat, murah, dan adil. Secara keseluruhan, akibat hukum dari kebocoran data terhadap peserta BPJS Ketenagakerjaan tidak dapat direduksi hanya sebagai gangguan sistemik. Ia adalah pelanggaran serius terhadap hak warga negara yang mencerminkan lemahnya sistem perlindungan hukum atas data pribadi di Indonesia. Negara harus segera membangun kerangka hukum dan kelembagaan yang berpihak pada korban, serta memastikan adanya akses terhadap keadilan dan kompensasi yang memadai, sebagai bentuk nyata penghormatan terhadap martabat manusia dalam era digital.

2. Akibat Hukum Bagi BPJS Ketenagakerjaan sebagai Pengendali Data (Data Controller)

Sebagai lembaga penyelenggara jaminan sosial nasional, BPJS Ketenagakerjaan memiliki tanggung jawab hukum yang besar dalam mengelola, menyimpan, dan melindungi data pribadi peserta. Dalam kerangka Undang-Undang Pelindungan Data Pribadi, BPJS Ketenagakerjaan dikategorikan sebagai pengendali data pribadi (data controller), yakni pihak yang menentukan tujuan dan kendali atas pemrosesan data pribadi. Dengan status tersebut, BPJS tidak hanya memiliki kewajiban administratif untuk mengelola data dengan aman, tetapi juga menanggung konsekuensi hukum apabila terjadi kebocoran data akibat kelalaian, kesengajaan, atau kegagalan sistemik. Akibat hukum yang dapat timbul terhadap BPJS Ketenagakerjaan meliputi pertanggungjawaban perdata, administratif, dan pidana, sebagaimana dijelaskan berikut ini:

a. Potensi Pertanggungjawaban Hukum

Dalam ranah hukum perdata, BPJS Ketenagakerjaan dapat dimintai pertanggungjawaban atas perbuatan melawan hukum (onrechtmatige daad) sebagaimana diatur dalam Pasal 1365 KUHPerdata, yang menyatakan:

"Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang karena kesalahannya menerbitkan kerugian itu, mengganti kerugian tersebut."

Jika dapat dibuktikan bahwa kebocoran data disebabkan oleh kelalaian dalam sistem keamanan BPJS, maka peserta yang dirugikan memiliki dasar untuk mengajukan gugatan ganti rugi perdata. Kelalaian BPJS—misalnya, dalam memperbarui sistem keamanan siber, gagal melakukan enkripsi data, atau membiarkan celah keamanan terbuka dapat dinilai sebagai

bentuk pelanggaran kewajiban hukum yang menimbulkan kerugian pada peserta. Hal ini membuka peluang bagi korban untuk mengajukan gugatan ke pengadilan guna memperoleh kompensasi, baik materiil maupun immateriil.

Di samping sanksi perdata, BPJS juga dapat dikenakan sanksi administratif sebagaimana diatur dalam Pasal 57 dan 58 UU PDP. Sanksi administratif ini bersifat berjenjang dan dapat dijatuhkan oleh otoritas pengawas pelindungan data (yang kewenangannya akan dibentuk melalui peraturan pelaksana UU PDP). Bentuk sanksi tersebut antara lain:

1. Teguran tertulis;
2. Penghentian sementara aktivitas pemrosesan data pribadi;
3. Penghapusan data pribadi;
4. Denda administratif, yang besarannya bisa mencapai 2% dari pendapatan tahunan atau penerimaan tahunan, tergantung pada tingkat pelanggaran yang terjadi.

Sanksi administratif ini penting sebagai bentuk kontrol negara terhadap pengendali data, sekaligus menjadi tekanan hukum agar BPJS tidak abai terhadap kewajiban perlindungan data peserta. Kegagalan dalam merespons insiden kebocoran data, atau tidak memberikan notifikasi kepada korban sesuai dengan kewajiban dalam UU PDP, juga termasuk pelanggaran administratif yang bisa dikenai sanksi tambahan.

Akibat hukum yang paling serius bagi BPJS Ketenagakerjaan muncul dalam bentuk pertanggungjawaban pidana, jika terbukti terjadi unsur kesengajaan atau kelalaian berat dalam pengelolaan dan perlindungan data pribadi. Hal ini diatur dalam Pasal 67 sampai dengan Pasal 73 UU PDP, yang menetapkan bahwa:

1. Setiap orang (termasuk badan hukum) yang secara melawan hukum mengakses, mengungkapkan, dan/atau menyebarluaskan data pribadi tanpa persetujuan subjek data dapat dipidana dengan penjara hingga 5 (lima) tahun dan/atau denda hingga Rp5 miliar.
2. Jika pelanggaran dilakukan oleh korporasi, seperti badan publik atau institusi, maka sanksi dapat diperluas meliputi:
   1) Pembayaran denda maksimal;
   2) Pencabutan izin usaha tertentu;
   3) Larangan sementara dalam pengolahan data pribadi;
   4) Penyitaan keuntungan yang diperoleh dari pemrosesan data pribadi yang melanggar hukum.

Meskipun BPJS adalah lembaga negara, ketentuan pidana dalam UU PDP tidak mengecualikan tanggung jawab pidana bagi badan publik. Hal ini menjadi bukti bahwa negara mengakui pentingnya kesetaraan tanggung jawab hukum dalam konteks pelindungan data pribadi. Dalam hal ditemukan bahwa pelanggaran terjadi karena kelalaian berat, seperti kegagalan memperbarui sistem keamanan atau penggunaan sistem pihak ketiga tanpa pengamanan yang layak, maka aparatur yang bertanggung jawab secara struktural dapat dikenakan pertanggungjawaban pidana secara individu (individual liability).

b. Tanggung Jawab Etis dan Moral

Di luar aspek yuridis yang mengatur sanksi perdata, administratif, dan pidana, BPJS Ketenagakerjaan sebagai institusi publik juga memikul tanggung jawab etis dan moral yang tidak kalah penting. Sebagai badan yang mengelola dan menghimpun data sensitif milik jutaan peserta, termasuk informasi identitas, pekerjaan, penghasilan, serta rekam jejak jaminan sosial, BPJS memiliki peran sentral dalam menjamin rasa aman dan kepercayaan publik terhadap sistem negara. Dalam konteks ini, tanggung jawab BPJS tidak hanya berhenti pada aspek kepatuhan hukum (legal compliance), tetapi juga mencakup akuntabilitas moral terhadap dampak sosial, psikologis, dan emosional yang dialami oleh peserta akibat kebocoran data pribadi.

Ketika terjadi kebocoran, banyak korban tidak hanya mengalami kerugian material, tetapi juga kerugian immaterial berupa rasa cemas, takut, dan terancam dalam menjalani aktivitas digital sehari-hari. Beberapa bahkan mengalami tekanan mental akibat menjadi korban phishing, scam, atau penyalahgunaan identitas tanpa memiliki instrumen perlindungan yang memadai. Dalam situasi seperti ini, sangat tidak etis apabila BPJS hanya bersikap reaktif, menutupi insiden, atau memberikan tanggapan formal tanpa empati. Sebagai lembaga publik, BPJS memiliki kewajiban moral untuk memulihkan martabat peserta sebagai warga negara, termasuk melalui langkah-langkah seperti:

1. Permintaan maaf secara terbuka dan resmi;
2. Menyediakan bantuan psikologis atau konseling bagi peserta terdampak;

3. Mengganti biaya-biaya administratif yang timbul akibat kerugian digital;
4. Menjamin non-repetisi (non-repetition guarantee), yaitu memastikan bahwa kejadian serupa tidak akan terulang di masa depan.

Tanggung jawab moral ini juga mencerminkan prinsip dasar pelayanan publik yang berorientasi pada kepentingan masyarakat, bukan semata-mata efisiensi administrasi atau kepatuhan prosedural. Dalam konteks negara hukum demokratis, etika publik menjadi fondasi legitimasi kelembagaan. Oleh karena itu, kegagalan dalam mengakui dan menanggapi kerugian non-yuridis peserta akan menjadi preseden buruk yang mencederai nilai-nilai keadilan sosial.

c. Keruntuhan Kepercayaan Publik dan Legitimasi Kelembagaan

Kebocoran data pribadi juga membawa konsekuensi sistemik yang berbahaya, yakni keruntuhan kepercayaan publik terhadap lembaga BPJS Ketenagakerjaan dan, secara lebih luas, terhadap sistem jaminan sosial negara. Dalam teori administrasi publik modern, kepercayaan adalah prasyarat utama bagi efektivitas kebijakan dan partisipasi warga. Ketika data pribadi yang dipercayakan pada institusi negara bocor dan tidak ditangani secara bertanggung jawab, maka secara perlahan akan terjadi "withdrawal trust" yakni gejala penarikan kepercayaan oleh peserta terhadap institusi.

Withdrawal trust ini bisa bermakna konkret, seperti:

1. Peserta enggan memperbarui data pribadi secara berkala karena takut terjadi kebocoran;
2. Peserta tidak lagi menggunakan layanan digital BPJS, seperti aplikasi JMO atau e-claim karena tidak percaya terhadap sistem keamanan digitalnya;
3. Munculnya desakan untuk menutup akun, menghapus data dari sistem, atau bahkan menarik diri dari sistem jaminan sosial secara keseluruhan, yang dalam jangka panjang dapat melemahkan basis kepesertaan aktif.

Fenomena ini sangat berbahaya karena BPJS sebagai sistem jaminan sosial berbasis gotong royong memerlukan partisipasi aktif dan keyakinan warga negara terhadap integritas sistemnya. Jika ketidakamanan data menjadi kebiasaan atau dianggap hal biasa, maka dampak domino-nya bukan hanya menurunkan efisiensi layanan, tetapi juga meruntuhkan legitimasi kelembagaan BPJS sebagai penyelenggara program publik. Terlebih lagi, dalam konteks negara yang tengah mendorong transformasi digital, kegagalan BPJS dalam menjamin keamanan data akan memperkuat narasi negatif bahwa pemerintah belum siap atau tidak layak mengelola ekosistem digital berskala besar. Hal ini dapat menghambat program digitalisasi nasional lainnya, termasuk di sektor kesehatan, pendidikan, dan perpajakan. Maka, keruntuhan kepercayaan publik bukan hanya merugikan BPJS secara langsung, tetapi juga menciptakan efek krisis legitimasi yang luas terhadap institusi negara.

Oleh karena itu, pemulihan kepercayaan tidak cukup dilakukan melalui pernyataan formal atau peningkatan teknis belaka. Diperlukan langkah reformasi menyeluruh, termasuk:

1. Transparansi insiden dan audit publik terhadap sistem perlindungan data;\
2. Keterlibatan lembaga independen dalam pengawasan BPJS;
3. Peningkatan literasi digital bagi peserta, serta
4. Pelibatan korban dalam penyusunan kebijakan pasca-insiden.

Allan F. Westin, mengemukakan bahwa privasi adalah hak individu untuk mengendalikan informasi pribadi mereka sendiri. Westin membagi privasi menjadi empat fungsi utama: solitude (kesendirian), intimacy (keintiman), anonymity (anonimitas), dan reserve (kerahasiaan). Menurut Westin dalam konteks kebocoran data pribadi BPJS Ketenagakerjaan karena insiden tersebut telah melanggar prinsip-prinsip dasar privasi.

Salah satu pilar utama dalam teori Westin adalah bahwa individu memiliki hak penuh atas informasi pribadi mereka, termasuk hak untuk menentukan siapa yang boleh mengakses, menggunakan, dan menyebarkan informasi tersebut. Dalam konteks BPJS Ketenagakerjaan, data peserta seperti NIK, alamat, nomor HP, status kepesertaan, dan data kerja merupakan data sensitif yang seharusnya tidak dapat diakses tanpa izin dari pemilik data. Ketika data ini bocor, BPJS Ketenagakerjaan telah gagal memenuhi prinsip kontrol individual atas data pribadi. Peserta tidak diberi ruang untuk menyetujui (informed consent) penggunaan data secara rinci, apalagi atas kebocorannya.

Fungsi intimacy dan reserve dalam teori Westin menekankan pentingnya menjaga informasi yang bersifat pribadi, personal, dan sensitif, termasuk kondisi pekerjaan, gaji, dan status kesehatan yang sering tercermin dalam data BPJS. Ketika informasi seperti ini bocor,

terjadi pengingkaran terhadap hak peserta untuk menyembunyikan atau membatasi akses terhadap informasi pribadi yang tidak ingin mereka ungkapkan kepada publik. BPJS sebagai institusi negara yang seharusnya melindungi kerahasiaan peserta justru berkontribusi secara tidak langsung terhadap pelanggaran fungsi reserve tersebut. Ini menunjukkan adanya kelalaian struktural dan kelembagaan, yang memperbesar beban psikologis peserta. Fungsi anonimity adalah kebebasan individu untuk menjalani kehidupan tanpa diawasi atau dilacak oleh pihak lain. Dalam insiden kebocoran data BPJS, data yang bocor membuka kemungkinan praktik pengawasan digital secara tidak sah oleh pihak ketiga, termasuk dalam bentuk phishing, penipuan pinjaman online, hingga social engineering. Peserta BPJS yang awalnya memiliki anonimitas digital kini terekspos secara luas, bahkan tanpa mereka sadari, keruntuhan anonimitas ini merupakan pelanggaran serius terhadap kebebasan sipil, karena individu tidak lagi dapat merasa aman dalam aktivitas digital maupun interaksi sosial.

Seharusnya lembaga publik memiliki tanggung jawab moral dan institusional untuk menjaga privasi warga negara melalui perangkat hukum dan teknis yang memadai. Dalam kasus BPJS Ketenagakerjaan, ketidakmampuan institusi ini untuk mencegah kebocoran data menunjukkan kegagalan perlindungan privasi secara sistemik, baik dari aspek keamanan digital, manajemen risiko, maupun tanggung jawab administratif. Lebih jauh lagi, keterlambatan pembentukan dan operasionalisasi otoritas pengawas perlindungan data pribadi sebagaimana diamanatkan UU PDP juga memperparah lemahnya sistem perlindungan tersebut. Peserta kehilangan mekanisme yang seharusnya bisa memberi perlindungan dan keadilan.

Dengan demikian, dapat disimpulkan bahwa kebocoran data peserta BPJS Ketenagakerjaan adalah pelanggaran berat terhadap hak atas privasi. Pelanggaran ini mencakup:

1. Gagalnya pengendalian atas data pribadi,
2. Pengingkaran terhadap hak untuk menjaga reserve dan anonimitas,
3. Ketidaksediaan mekanisme perlindungan institusional yang adil,
4. serta hilangnya pilihan bebas dari peserta dalam relasi data.

Implikasi ini tidak hanya bersifat hukum, tetapi juga moral dan sosial, mengharuskan adanya reformasi besar dalam sistem perlindungan data, tata kelola digital, serta akuntabilitas institusional di sektor pelayanan publik di Indonesia.

Teori perlindungan hukum, sebagaimana dikembangkan oleh Philipus M. Hadjon, menyatakan bahwa perlindungan hukum bagi warga negara adalah segala upaya untuk memberikan rasa aman kepada masyarakat dari ancaman pelanggaran hak, termasuk oleh negara. Perlindungan hukum tidak hanya bersifat represif (penyelesaian sengketa) tetapi juga preventif (pencegahan terjadinya pelanggaran hak). Dalam konteks data pribadi, hak atas perlindungan data merupakan hak konstitusional yang dijamin oleh Pasal 28G ayat (1) UUD 1945, sehingga setiap pelanggaran terhadap data pribadi dapat dimaknai sebagai pelanggaran terhadap hak asasi manusia.

Kebocoran data pribadi peserta BPJS Ketenagakerjaan merupakan bentuk nyata dari kegagalan negara (melalui lembaga publik seperti BPJS) dalam memberikan perlindungan hukum. Berdasarkan teori perlindungan hukum, hak atas data pribadi adalah hak subjektif yang melekat pada setiap individu dan wajib dihormati oleh negara maupun entitas lain. Ketika data pribadi peserta bocor dan dimanfaatkan oleh pihak ketiga untuk tindakan ilegal (seperti penipuan atau pencurian identitas), maka peserta mengalami kerugian secara langsung. Dalam hal ini, negara wajib menyediakan mekanisme remedial hukum yang adil, cepat, dan efektif.

Namun, dalam praktiknya, mekanisme ini masih lemah. Sebagai contoh, meskipun UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah menjamin hak-hak subjek data seperti hak atas akses, hak untuk memperbaiki, dan hak untuk menghapus data, implementasinya belum optimal karena lembaga pengawas independen yang dijanjikan UU tersebut (yakni Badan Pengawas PDP) masih belum terbentuk secara fungsional. Hal ini mengakibatkan peserta tidak memiliki saluran yang pasti untuk menuntut ganti rugi atau pemulihan atas haknya, sehingga mencerminkan lemahnya perlindungan hukum secara de facto meskipun secara de jure sudah ada aturan hukum.

Dari sisi institusi penyelenggara, teori perlindungan hukum mengandung prinsip bahwa badan publik juga tunduk pada prinsip akuntabilitas hukum. BPJS Ketenagakerjaan sebagai pengendali data wajib melaksanakan prinsip kehati-hatian dalam mengelola dan menyimpan data pribadi peserta. Dalam konteks ini, jika BPJS lalai dalam pengamanan data hingga terjadi kebocoran, maka institusi tersebut dapat dimintai pertanggungjawaban hukum. UU PDP telah

mengatur sanksi administratif dan pidana terhadap pelanggaran pengendali data, termasuk tidak menerapkan sistem pengamanan yang memadai atau tidak melaporkan insiden kebocoran data. Ini adalah bentuk perlindungan hukum dalam ranah administratif dan pidana. Namun lagi-lagi, secara praktis belum terlihat adanya penegakan hukum yang tegas terhadap BPJS atau lembaga publik lain yang datanya bocor. Artinya, meskipun perlindungan hukum secara normatif tersedia, efektivitas penerapannya belum menunjukkan kekuatan sebagai alat kontrol terhadap institusi negara.

Di sisi lain, perlindungan hukum terhadap BPJS sebagai institusi juga harus dipahami dalam kerangka yang seimbang. BPJS juga menjadi pihak yang perlu dilindungi dari tekanan atau serangan yang tidak proporsional selama masih bertindak sesuai prinsip hukum dan menunjukkan itikad baik dalam menyelesaikan insiden kebocoran data. Namun, jika kelalaian terbukti, maka perlindungan hukum tidak boleh berubah menjadi bentuk impunitas institusional.

Berdasarkan teori perlindungan hukum, sistem hukum harus mampu menjamin kepastian hukum, keadilan, dan manfaat. Ketiga prinsip ini diuji dalam kasus kebocoran data BPJS Ketenagakerjaan:

Kepastian hukum

Secara normatif, telah tersedia dalam UU PDP, UU ITE, dan sejumlah regulasi teknis. Namun, implementasinya masih belum jelas, karena lemahnya penegakan dan ketiadaan lembaga pengawas independen yang efektif.

Keadilan

Belum sepenuhnya tercapai karena peserta yang menjadi korban kebocoran belum mendapatkan kompensasi yang layak, baik secara administratif maupun perdata. Mekanisme penyelesaian sengketa juga belum jelas dan aksesibilitasnya rendah.

Kemanfaatan

Perlindungan hukum belum memberi efek jera atau pencegahan yang nyata terhadap terulangnya pelanggaran. Ini menunjukkan perlunya perbaikan struktural dan prosedural dalam penanganan kebocoran data.

D. Kesimpulan

Kebocoran data pribadi peserta BPJS Ketenagakerjaan menimbulkan akibat hukum yang kompleks dan berlapis, baik bagi peserta sebagai subjek data maupun bagi BPJS Ketenagakerjaan sebagai pengendali data. Bagi peserta, kebocoran data telah mengakibatkan pelanggaran serius atas hak privasi yang dijamin oleh konstitusi dan dijabarkan secara eksplisit dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Hak atas perlindungan data pribadi merupakan bagian dari hak atas rasa aman, sebagaimana dijamin oleh Pasal 28G ayat (1) UUD 1945, sehingga setiap pelanggaran terhadapnya dapat dikualifikasikan sebagai pelanggaran hak konstitusional. Selain itu, kebocoran data menimbulkan potensi penyalahgunaan yang signifikan, seperti penipuan digital, pemalsuan identitas, hingga pencurian data yang berdampak langsung pada keamanan sosial, psikologis, dan ekonomi peserta. Potensi tersebut menciptakan kerugian nyata dan potensial yang dapat dijadikan dasar gugatan perdata berdasarkan Pasal 1365 KUHPerdata tentang perbuatan melawan hukum, di mana peserta berhak menuntut ganti rugi terhadap BPJS sebagai pengendali data atas kelalaian yang menyebabkan kerugian tersebut.

Bagi institusi BPJS Ketenagakerjaan, kebocoran data menciptakan kewajiban hukum untuk bertanggung jawab, baik dalam ranah perdata, administratif, maupun pidana apabila ditemukan unsur kesengajaan atau kelalaian berat. Pertanggungjawaban perdata dapat dikenakan berdasarkan prinsip *strict liability* sebagaimana berkembang dalam rezim hukum perlindungan data modern, di mana pengendali data tetap bertanggung jawab meskipun tidak terbukti lalai secara subjektif. Selain itu, BPJS berpotensi dijatuhi sanksi administratif berdasarkan Pasal 57 ayat (2) UU PDP, yang meliputi teguran, denda administratif, pembekuan kegiatan pengolahan data, hingga pemutusan akses sistem. Parameter penjatuhan sanksi mempertimbangkan derajat kelalaian, dampak kebocoran, serta jumlah data yang terdampak. Secara pidana, apabila ditemukan unsur kesengajaan atau kelalaian berat, institusi dan individu di dalamnya dapat dikenakan sanksi berdasarkan Pasal 67 dan Pasal 68 UU PDP, serta dapat dikaitkan pula dengan ketentuan pidana dalam UU ITE yang mengatur kejahatan terhadap sistem elektronik.Di sisi lain, kebocoran data juga menimbulkan kewajiban hukum bagi BPJS

untuk melakukan notifikasi kepada peserta sebagaimana diatur dalam Pasal 46 UU PDP, yang mengharuskan pemberitahuan segera apabila terjadi pelanggaran data. Kegagalan atau kelalaian dalam menyampaikan notifikasi dapat mengakibatkan sanksi tambahan dan memperburuk kerugian yang dialami peserta. Kebocoran data juga berdampak pada aspek non-hukum seperti reputasi institusi, kepercayaan publik, dan legitimasi lembaga penyelenggara jaminan sosial. Risiko jangka panjang mencakup penurunan partisipasi digital, resistensi masyarakat terhadap digitalisasi layanan publik, serta meningkatnya beban administratif dalam pemulihan dan penguatan sistem keamanan data. Oleh karena itu, urgensi reformasi kelembagaan dan peningkatan standar pengamanan data menjadi bagian penting dari konsekuensi hukum dan institusional dari insiden ini. Keseluruhan akibat hukum ini menunjukkan bahwa perlindungan data pribadi tidak hanya merupakan isu teknis, tetapi menyangkut keadilan, kepastian hukum, dan akuntabilitas penyelenggara layanan publik di era digital.

Saran

Agar BPJS Ketenagakerjaan dapat mengembangkan dan memperkuat sistem keamanan siber, termasuk penggunaan enkripsi data, firewall, sistem deteksi intrusi (IDS), dan pengamanan berbasis AI untuk mendeteksi dan menangkal ancaman lebih awal, dan memberikan pelatihan intensif dan berkelanjutan kepada seluruh pegawai, khususnya yang mengelola sistem informasi, tentang prinsip-prinsip keamanan data pribadi dan tata kelola data sesuai dengan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta peserta BPJS harus dapat memahami pentingnya perlindungan data pribadi dan secara aktif mengikuti edukasi atau informasi yang diberikan BPJS tentang cara melindungi identitas dan informasi pribadi mereka, serta perlu waspada terhadap upaya penipuan yang mengatasnamakan BPJS, seperti permintaan data melalui tautan tidak resmi, dan tidak memberikan data pribadi melalui saluran yang tidak jelas keasliannya.

E. Referensi

Alan F. Westin, (1967) Privacy and Freedom, New York: Atheneum.
Badan Siber dan Sandi Negara (BSSN) 2023, “Laporan Keamanan Siber Nasional.”
BPJS Ketenagakerjaan, Laporan Tahunan 2022,
CNN Indonesia, “Data Peserta BPJS Ketenagakerjaan Dijual Lagi di Forum Hacker?”.
CNN Indonesia, “Hacker Bjorka Klaim Bobol 19 Juta Data BPJS Ketenagakerjaan”.
Daniel J. Solove, Understanding Privacy (Harvard University Press, 2006)
Komnas HAM, Laporan Hak Atas Privasi dan Perlindungan Data Pribadi, 2022.
Kompas.com, "Data 279 Juta Penduduk Indonesia Diduga Bocor dan Dijual, Kominfo Lakukan Penelusuran".
Kompas.com, “Masyarakat Masih Khawatir Meski BPJS Klaim Data Aman,” 2023
Laporan Insiden Kebocoran Data BPJS Ketenagakerjaan, Kominfo, 2023.
P. Agustina, “Perlindungan Hukum Data Pribadi di Indonesia,” Jurnal Hukum & Pembangunan, Vol. 49 No. 1, 2019.
Peraturan Pemerintah Nomor 44 Tahun 2015 tentang Penyelenggaraan Program Jaminan Kecelakaan Kerja dan Jaminan Kematian.
Peraturan Perundang-undangan
Phillipus M. Hadjon, Perlindungan Hukum bagi Rakyat di Indonesia (Surabaya: Bina Ilmu, 1987).
Samuel D. Warren dan Louis D. Brandeis, “The Right to Privacy,” Harvard Law Review 4, no. 5 (1890).
Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggara Jaminan Sosial.
Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
Website