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

Analisis Keamanan Data Pribadi Konsumen terhadap Regulasi Pencantuman Nomor Induk Kependudukan untuk Registrasi Nomor Telepon

INFO PENULIS

Mario Alvember
Universitas Esa Unggul Jakarta
marioalvember@gmail.com

Dyah Permata Budi Asri
Universitas Esa Unggul Jakarta
dyah.permata@esaunggul.ac.id

INFO ARTIKEL

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

Saran Penulisan Referensi:

Alvember, M., & Asri, D. P. B. (2025). Analisis Keamanan Data Pribadi Konsumen terhadap Regulasi Pencantuman Nomor Induk Kependudukan untuk Registrasi Nomor Telepon. *Arus Jurnal Sosial dan Humaniora, 5*(2), 3017-3026.

Abstrak

Era Revolusi Industri 4.0 telah mendorong transformasi digital yang mendalam di Indonesia, membuat koneksi internet dan perangkat digital menjadi kebutuhan utama dalam berbagai aspek kehidupan. Namun, kemajuan ini membawa tantangan serius terkait keamanan data pribadi konsumen, terutama dalam konteks regulasi pencantuman Nomor Induk Kependudukan (NIK) untuk registrasi nomor telepon. Data pribadi seperti NIK merupakan data sensitif yang rentan disalahgunakan jika tidak dikelola dengan baik. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi payung hukum utama yang mengatur pengelolaan, hak subjek data, serta kewajiban dan tanggung jawab penyelenggara layanan dalam melindungi data pribadi. Implementasi UU PDP menuntut provider telekomunikasi untuk membangun sistem keamanan yang andal, menggunakan teknologi seperti Data Loss Prevention (DLP) guna mencegah kebocoran, serta menjalankan prinsip transparansi dan akuntabilitas. Perlindungan data pribadi tidak hanya penting untuk melindungi konsumen dari risiko penyalahgunaan dan kerugian, tetapi juga menjadi fondasi kepercayaan yang mendukung perkembangan ekonomi digital yang inklusif dan berkelanjutan. Meskipun kerangka hukum telah ada, tantangan implementasi dan edukasi masyarakat masih signifikan. Oleh karena itu, sinergi antara regulasi, teknologi, dan kesadaran masyarakat sangat diperlukan untuk memastikan perlindungan data pribadi yang efektif dalam era digital yang terus berkembang. Penelitian ini bertujuan menganalisis tanggung jawab provider dalam melindungi data pribadi konsumen dan efektivitas UU PDP sebagai upaya perlindungan hukum atas data pribadi konsumen di Indonesia.

Kata Kunci: Perlindungan Hukum; Data Pribadi ; Registrasi Kartu Prabayar.

Abstract

The Industrial Revolution 4.0 era has driven a profound digital transformation in Indonesia, making internet connections and digital devices essential for various aspects of life. However, this progress presents serious challenges related to the security of consumers' personal data, particularly in the context of regulations regarding the inclusion of Population Identification Numbers (NIK) for telephone number registration. Personal data, such as NIKs, is sensitive and vulnerable to misuse if not managed properly. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) serves as the primary legal umbrella governing the management, rights of data subjects, and the obligations and responsibilities of service providers in protecting personal data. Implementation of the PDP Law requires telecommunications providers to build reliable security systems, utilize technologies such as Data Loss Prevention (DLP) to prevent leaks, and uphold the principles of transparency and accountability. Personal data protection is not only crucial for protecting consumers from the risk of misuse and loss, but also serves as a foundation of trust that supports the development of an inclusive and sustainable digital economy. Despite the existing legal framework, significant challenges remain in implementation and public education. Therefore, synergy between regulation, technology, and public awareness is essential to ensure effective personal data protection in the evolving digital era. This study aims to analyze providers' responsibilities in protecting consumers' personal data and the effectiveness of the Personal Data Protection Law as a legal protection measure for consumer personal data in Indonesia.

Keywords: Legal Protection; Personal Data; Prepaid Card Registration

A. Pendahuluan

Sejak memasuki era Revolusi Industri 4.0, segala aktivitas sehari-hari di Indonesia semakin bergantung pada koneksi internet dan perangkat digital. Kemudahan dalam mengendalikan sistem dari jarak jauh telah mendorong perubahan signifikan dalam berbagai aspek kehidupan: produktivitas tenaga kerja meningkat, interaksi sosial-ekonomi semakin dinamis, dan beragam layanan menjadi lebih praktis. Kehadiran smartphone dan teknologi informasi-komunikasi tidak hanya mengubah gaya hidup, tetapi juga memunculkan pola budaya baru serta memengaruhi bidang pertahanan, keamanan, penegakan hukum, dan ekonomi masyarakat (Wiryany et al.)

Keamanan data pribadi konsumen merupakan aspek penting dalam transaksi, terutama di era digital dan e-cormmerce. Perlindungan data pribadi konsumen bertujuan melindungi privasi, keamanan, dan hak konsumen agar data tidak disalahgunakan atau bocor ke pihak tak berwenang. Secara keseluruhan, permasalahan utama adalah bagaimana memastikan keamanan dan keabsahan data pribadi konsumen dalam proses registrasi nomor telepon, mencegah penyalahgunaan NIK, serta menjaga keseimbangan antara perlindungan data pribadi dan kebutuhan regulasi telekomunikasi yang efektif.

Pencantuman NIK dalam registrasi nomor telepon menimbulkan kekhawatiran terkait keamanan dan perlindungan data pribadi konsumen. NIK yang bersifat unik dan permanen menjadi data sensitif yang Tanpa dikelola dengan baik dapat berpotensi disalahgunakan, mengancam privasi dan keamanan konsumen. Oleh karena itu, penting untuk mengevaluasi keamanan data pribadi konsumen dalam konteks regulasi ini, guna memastikan bahwa perlindungan data pribadi konsumen dijaga agar sesuai dengan prinsip perlindungan konsumen dan hukum yang berlaku. ini juga relevan mengingat pesatnya kemajuan teknologi informasi dan tingginya kebutuhan perlindungan data pribadi di era digital. Dengan demikian, kajian terhadap regulasi pencantuman NIK dalam registrasi nomor telepon menjadi krusial untuk menyeimbangkan antara kebutuhan administrasi publik dan hak konsumen atas keamanan data pribadinya.

Pada dunia kerja, kemampuan mengelola data dalam jumlah masif secara cepat dan tepat membawa efisiensi tinggi serta meminimalisir kesalahan. Berdasarkan pada aspek bisnis, digitalisasi mempermudah promosi dan memperluas jangkauan pasar melampaui batas-batas geografis, baik lokal, regional, maupun global sehingga peluang peningkatan kesejahteraan masyarakat dapat terwujud dengan lebih cepat. Sementara itu, kemajuan ilmu pengetahuan dan teknologi memberi akses informasi dalam skala yang sangat luas dan dalam cakupan yang tak pernah tercapai sebelumnya, menghasilkan miliaran bahkan triliunan data yang dapat dianulir untuk berbagai kepentingan.

Hingga kini, regulasi perlindungan data di Indonesia tersebar di berbagai undang-undang dan peraturan sektoral, tanpa payung hukum tunggal yang komprehensif. Sebagian besar acuan

hukum masih merujuk pada Pasal 28G UUD 1945 yang secara substansial menjamin prerogatif individu terhadap proteksi atas integritas diri, unit keluarga, respek sosial, harga diri, serta rasa aman dari intimidasi dan teror psikologis. Belum adanya satu kesatuan regulasi yang terfokus membuat penerapan prinsip-prinsip tersebut dalam praktik seringkali belum optimal, sehingga memunculkan celah bagi pelanggaran data pribadi yang merugikan masyarakat (Nafi'ah, 2020).

Di Indonesia, regulasi terhadap data privat individu masih diimplementasikan secara fragmentaris melalui berbagai legislasi sektoral, dan belum ada payung hukum tunggal yang komprehensif UU No. 27 Tahun 2022 Mengenai Perlindungan Data Pribadi (UU PDP). merepresentasikan artikulasi yuridis yang signifikan dalam menyusun struktur secara eksplisit mengenai klasifikasi data personal, prerogatif entitas data, serta tanggung jawab entitas pengendali data. Regulasi ini mencakup sanksi bagi pelanggar dan pembentukan badan pengawas independen demi efektivitas perlindungan data. Namun, tantangan implementasi masih besar, terutama dalam hal edukasi masyarakat dan penguatan mekanisme pengawasan.

Selain itu, perkembangan teknologi informasi yang pesat juga meningkatkan risiko kebocoran data pribadi, termasuk NIK, yang dapat dimanfaatkan oleh aktor jahat digital. Oleh karena itu, konsumen dan masyarakat diimbau untuk meningkatkan kesadaran dan langkah-langkah perlindungan data pribadi secara mandiri, seperti menjaga kerahasiaan data dan waspada terhadap penipuan yang semakin canggih.

Lebih jauh, peningkatan penggunaan layanan digital dan transaksi elektronik membuka peluang sekaligus risiko di berbagai sektor kehidupan, mulai dari bisnis, pemerintahan, hingga sosial budaya. Efisiensi yang diperoleh dari pengelolaan data secara cepat dan akurat harus diimbangi dengan kewaspadaan terhadap potensi pelanggaran privasi dan penyalahgunaan data. Pengaturan tata kelola dan perlindungan data pribadi tidak hanya diposisikan sebagai penjamin kepastian hukum, tetapi juga dipercaya membangun kepercayaan publik terhadap ekosistem digital nasional. Dengan demikian, perlindungan data pribadi dipandang sebagai landasan utama dalam mendorong ekonomi digital yang inklusif dan terus berkembang.

Langkah konkret telah diambil oleh pemerintah melalui Peraturan Menteri Komunikasi dan Informatika No. 12 Tahun 2016 terkait registrasi pelanggan jasa telekomunikasi, yang kemudian diubah melalui Peraturan Menteri Komunikasi dan Informatika No. 21 Tahun 2017, sebagai upaya memperbaiki proses registrasi dan meningkatkan perlindungan data konsumen dalam sektor telekomunikasi. Regulasi ini mengatur tata cara pencantuman data pribadi termasuk NIK dalam registrasi nomor telepon, sekaligus menegaskan tanggung jawab penyelenggara jasa telekomunikasi dalam menjaga kerahasiaan dan keamanan data pelanggan. Dengan demikian, sinergi antara peraturan sektoral dan UU PDP diharapkan berpotensi membangun sistem perlindungan data pribadi yang tangguh dan efisien di Indonesia.

Rumusan Masalah

Berdasarkan fokus utama skripsi dan struktur hukum tata negara, berikut rumusan masalah yang lebih terarah:

1. Bagaimana tanggung jawab pihak provider dalam melindungi data pribadi konsumen jika ada kebocoran data pribadi?
2. Apakah Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dapat memberikan perlindungan bagi konsumen?

B. Metodologi

Penelitian ini merupakan kegiatan ilmiyah untuk memahami atau mempelajari faktor faktor yang baru, yang memerlukan metode penelitian yakni:

1. Jenis dan Sifat Penelitian

Penelitian ini diklasifikasikan sebagai studi hukum normatif melalui pendekatan yuridis-normatif berfokus pada analisis norma tertulis yang mengatur registrasi SIM prabayar berbasis NIK dan KK, dengan menelaah maksud pembentukan undang-undang serta kerangka konseptual perlindungan data pribadi "Analisis Keamanan Data Pribadi Konsumen Terhadap Regulasi Pencantuman Nik Untuk Registrasi Nomor Telepon",

2. Data dan Sumber Data

Penulis menggunakan sumber data sekunder yang dikategorikan menjadi 3 antara lain:

1. Bahan Hukum Primer adalah bahan yang memaksa serta mengikat dalam masalah yang akan ditangani, yang mana bahan hukum utama bersumber dari undang-undang:
   a) UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi
   b) Undang-Undang Dasar 1945
   c) UU No. 19/2016 tentang Informasi dan Transaksi Elektronik

2. Bahan Hukum Sekunder
   Peneliti menerapkan bahan hukum sekunder dari sumber yang menjelaskan secara detail terkait bahan hukum primer, bahan hukum sekunder meliputi beberapa jurnal akademis dan buku menurut ahli yang berkaitan dengan topik pengaturan hukum akibat kebocoran data pribadi
3. Bahan Hukum Tersier
   Bahan hukum tersier diterapkan oleh peneliti mencangkup sumber sumber yang memberi arahan serta uraian terkait dengan bahan hukum sekunder, sebagai sumber hukum tersier, Peneliti melakukan studi kepustakaan *(library research)* melalui pengumpulan dan menelaah dokumen perundang-undangan, peraturan pelaksana, serta literatur akademik.

3. Alat Pengumpulan Data

Bahan hukum dianalisis secara deskriptif dan analitis melalui *content analysis* pasal-pasal inti (khususnya prinsip persetujuan dalam UU PDP), diikuti penafsiran sistematis (gramatikal, historis, dan teleologis).

4. Analisis Data dan Metode Penarikan Kesimpulan

Pada penelitian ini Teknik analisis yang diterapkan oleh penulis yaitu Teknik analisis kualitatif. Penelitian hukum kualitatif itu sendiri menekankan pada pengelolaan data dari bahan hukum primer dan sekunder pada penulisan nya mengedepankan analisis normative untuk kesesuaian norma dalam konteks tertentu, analisis ini melibatkan dokumen hukum dan jurnal serta buku akademis untuk mengkaji argument serta presfektif yang dapat menambah wawasan mengenai PENGATURAN HUKUM AKIBAT KEBOCORAN DATA, sehingga menghasilkan Kesimpulan dan data data yang berbasis bukti yang jelas

C. Hasil dan Pembahasan

Tanggung Jawab Pihak Provider Melindungi Data Pribadi Konsumen

Menurut Munir Fuady, setiap individu, termasuk entitas negara, diwajibkan untuk mengafirmasi akuntabilitas atas setiap perbuatannya, terlepas dari eksistensi kesalahan atau tidak. Berdasarkan konsepsi yuridis umum tersebut, lahirlah ragam pertanggungjawaban hukum seperti penal, perdata, dan administratif (Hufron, 2022).

Menurut Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022, data pribadi adalah informasi tentang individu yang dapat dikenali, baik langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik. Pengertian ini mencakup informasi yang secara eksplisit menyebut identitas seseorang seperti nama, NIK, atau alamat, serta informasi lain yang bila digabungkan dapat mengarah pada identifikasi individu, seperti lokasi, riwayat transaksi, atau data biometrik. UU PDP turut mengkategorisasikan informasi personal ke dalam dua klasifikasi, yakni data personal generik dan data personal distingtif (sensitif) seperti data kesehatan, keuangan, dan rekam jejak kriminal, yang memiliki tingkat kerahasiaan dan perlindungan yang lebih tinggi. Dengan demikian, setiap pihak yang memproses data pribadi wajib menjaga keamanan dan kerahasiaannya sesuai prinsip pelindungan data agar tidak terjadi penyalahgunaan yang merugikan subjek data.

Dalam kaitannya dengan perlindungan konsumen, hal ini berarti pihak penyedia layanan harus menjalankan kewajiban tersebut guna menjamin kepastian hukum dan perlindungan hak konsumen. Perlindungan konsumen merupakan segala upaya untuk memberikan jaminan keamanan, keadilan, dan kepastian hukum bagi konsumen agar terhindar dari tindakan sewenang-wenang yang merugikan (Mahameru et al.).

Melalui Undang-Undang No. 27 Tahun 2022 tentang perlindungan data pribadi, Indonesia telah memiliki dasar hukum yang kuat untuk melindungi data pribadi konsumen. UU ini mengatur secara rinci berbagai aspek, meliputi asas, tipe data, hak pemilik data, kewajiban pemrosesan, alur transfer, hingga sanksi dan penyelesaian sengketa. Tujuan utama UU PDP adalah mencegah terjadinya kebocoran data masyarakat serta menciptakan sistem yang efektif dan efisien dalam memberikan pelayanan, sekaligus menjamin perlindungan hukum bagi data pribadi konsumen.

Melalui penerapan DLP, risiko pengiriman data ke pihak yang tidak berwenang dapat ditekan, terutama terkait informasi rahasia perusahaan dan data pribadi milik konsumen, pegawai, maupun pihak ketiga (Vania et al.)

Layanan Data *Loss Prevention (DLP)* adalah strategi dan kumpulan alat yang dirancang untuk memastikan bahwa data sensitif dalam sebuah organisasi tidak hilang, bocor, atau disalahgunakan oleh pihak yang tidak berwenang. *DLP* bertujuan untuk memantau, mendeteksi, dan memblokir akses atau transfer data sensitif dari sistem perusahaan ke luar jaringan atau ke

pengguna yang tidak memiliki izin. Data yang dilindungi oleh *DLP* bisa berupa informasi pribadi, data keuangan, data pelanggan, data karyawan, atau data rahasia perusahaan lainnya.

Layanan Data *Loss Prevention (DLP)* yang berfungsi untuk mencegah kebocoran data dengan memantau dan mengontrol penggunaan data, serta memberikan peringatan jika ada aktivitas mencurigakan. Layanan ini juga mendukung pemenuhan standar keamanan seperti *ISO 27001, GDPR*. *provider* memang memiliki sistem keamanan data internal yang terdiri dari teknologi, prosedur, dan tenaga ahli keamanan untuk melindungi data konsumen dan aset digital mereka secara menyeluruh dan terstruktur. Sistem ini terus diperbaharui dan diperkuat sesuai dengan standar keamanan dan regulasi yang berlaku.

Pencegahan pengiriman data ke pihak tak berwenang merupakan fungsi utama DLP, yang memastikan data sensitif hanya diakses oleh pihak berwenang. Jika karyawan mencoba mengirim data penting ke luar, sistem akan langsung memblokirnya.

Dalam era digital saat ini, perlindungan tersebut tidak lepas dari tanggung jawab pelaku usaha termasuk *provider* layanan dalam melindungi data pribadi konsumen. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mengatur secara rinci mengenai asas, hak, jenis data, pemrosesan, transfer, hingga sanksi terkait perlindungan data pribadi. UU ini diciptakan guna mencegah kebocoran data dan memvalidasi pengelolaan data pribadi dilakukan secara aman dan bertanggung jawab. Misalnya, Pasal 16 ayat 2 huruf e UU PDP mewajibkan pemrosesan data pribadi dilakukan dengan menjaga keamanannya dari akses atau pengungkapan yang tidak sah, penyalahgunaan, perubahan, perusakan, hingga penghilangan data tersebut (Kadek Reza Ayuning Pranindya).

Penerapan UU PDP oleh penyedia layanan menjadi kunci membangun dan menjaga kepercayaan konsumen. Kepercayaan ini merupakan fondasi utama agar hubungan antara *provider* dan konsumen dapat berlangsung harmonis dan konsisten. Ketika konsumen merasa data pribadinya terlindungi dengan baik, mereka akan merasa nyaman serta loyal menggunakan produk atau layanan tersebut. Sebaliknya, ketidakpercayaan akibat pengelolaan data yang buruk dapat menimbulkan ketidaknyamanan, kekecewaan, bahkan merusak reputasi penyedia layanan.

Menurut Alan F. Westin sebagaimana disebut dalam teori ini menegaskan bahwa setiap individu berhak mengontrol informasi pribadi mengenai dirinya, termasuk siapa yang boleh mengakses dan memproses data tersebut. Penerapan teori ini membantu menilai sejauh mana asas persetujuan dalam Pasal Undang-Undang PDP memadai untuk memberi kontrol kepada subjek data atas NIK dan nomor HP mereka (Kusnadi, 2021).

Selanjutnya, Pasal 4 Undang-Undang nomor 8 tahun 1999 tentang perlindungan konsumen menegaskan hak konsumen yang wajib dijamin pelaku usaha, seperti hak atas kenyamanan, keamanan, informasi yang jelas, serta hak menyampaikan pendapat dan pengaduan. Konsumen turut memiliki legitimasi untuk mendapatkan pendampingan hukum, jaminan proteksi, serta resolusi konflik yang berkeadilan, termasuk restitusi apabila terjadi pelanggaran terhadap hak-haknya. Oleh karena itu, tanggung jawab provider tidak hanya sebatas memberikan layanan, tetapi juga memastikan hak-hak konsumen terpenuhi sesuai ketentuan hukum yang berlaku.

Sejalan dengan kewajiban provider, konsumen sebagai subjek data pribadi memiliki berbagai hak yang dijamin oleh UU PDP dan peraturan terkait lainnya. Hak-hak tersebut mencakup otoritas untuk memperoleh informasi, melakukan akses, merevisi, meniadakan, membatasi pemanfaatan, serta mentransfer data personal yang diadministrasikan oleh entitas eksternal. Konsumen pun memiliki legitimasi untuk menyampaikan keberatan atau pengaduan apabila data personal mereka digunakan secara ilegal atau bertentangan dengan regulasi.

Jika terjadi pelanggaran atau kebocoran data, UU PDP telah mengatur mekanisme pertanggungjawaban. Entitas pengendali data personal diwajibkan untuk memikul tanggung jawab atas prosesualisasi Data Pribadi serta mendemonstrasikan akuntabilitas terhadap pelaksanaan prinsip-prinsip Proteksi Data Personal, sebagaimana disebutkan dalam Pasal 47 UU PDP. Tanggung jawab ini bersifat *strict liability*, artinya perusahaan sebagai pengumpul data tetap memegang tanggung jawab utama meskipun pelaku langsungnya adalah pihak ketiga. Ini menegaskan pentingnya bagi perusahaan untuk melakukan *due diligence* dan pengawasan ketat terhadap mitra kerja yang memiliki akses data.

Kebocoran data pribadi memiliki konsekuensi yang luas, tak semata-mata merugikan konsumen namun turut mencoreng reputasi dan kredibilitas provider. Bagi konsumen, kebocoran data dapat menyebabkan kerugian finansial akibat penipuan, gangguan privasi, hingga tekanan psikologis. Sementara bagi provider, insiden kebocoran data dapat mengakibatkan denda yang besar, hilangnya kepercayaan pelanggan, penurunan nilai saham, dan biaya pemulihan yang signifikan.

Untuk memitigasi risiko ini, *provider* perlu mengimplementasikan standar keamanan yang ketat. Ini mencakup enkripsi data pribadi saat disimpan, penggunaan sistem pengamanan yang canggih untuk mencegah akses tidak sah, serta memastikan bahwa informasi pribadi tidak dikirim ke luar negeri tanpa jaminan perlindungan yang setara. Selain itu, edukasi dan sosialisasi kepada konsumen mengenai hak-hak mereka juga penting, seiring dengan peningkatan literasi digital di masyarakat. Implementasi *Non-Disclosure Agreement (NDA)* juga krusial untuk memastikan bahwa semua pihak dengan akses terhadap data, baik internal maupun eksternal, sehingga mencegah kebocoran akibat kelalaian atau tindakan oknum.

Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa setiap pengendali data pribadi memiliki kewajiban hukum untuk menjaga kerahasiaan data pribadi yang berada di bawah penguasaannya, dan dilarang mengungkapkan data tersebut kepada pihak lain tanpa persetujuan subjek data atau dasar hukum yang sah. Ketentuan ini secara langsung berkaitan dengan tanggung jawab penyelenggara sistem elektronik atau penyedia layanan *(provider)*, khususnya dalam melindungi data pribadi konsumen yang mereka himpun, simpan, dan olah dalam operasionalnya. *Provider* wajib memastikan bahwa sistem keamanannya mampu mencegah kebocoran, penyalahgunaan, atau akses ilegal terhadap data konsumen. Selain itu, *provider* juga bertanggung jawab untuk menerapkan prinsip transparansi, akuntabilitas, dan perlindungan privasi, termasuk memberikan pemberitahuan jika terjadi insiden pelanggaran data. Kegagalan dalam menjalankan tanggung jawab ini dapat berujung pada sanksi administratif maupun pidana sebagaimana diatur pada UU PDP, sehingga tugas provider guna melindungi data pribadi konsumen bukan hanya kewajiban etis, tetapi juga kewajiban hukum yang bersifat mengikat.

Tanggung jawab *provider* untuk menjaga data pribadi konsumen merupakan unsur krusial tak cuma bersandar kepada etika bisnis, namun pun telah diatur secara tegas dalam kerangka hukum nasional, khususnya melalui Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi serta Undang-Undang Nomor 8 Tahun 1999 mengenai Perlindungan Konsumen. Dalam era digital yang sarat akan risiko kebocoran dan penyalahgunaan data, *provider* dituntut untuk membangun sistem pengamanan yang andal, menerapkan prinsip kehati-hatian, serta menjamin penghormatan terhadap hak-hak konsumen sebagai subjek data. Kepatuhan terhadap ketentuan perundang-undangan tidak hanya melindungi konsumen dari potensi kerugian, tetapi juga menjadi fondasi bagi keberlanjutan hubungan bisnis yang sehat dan terpercaya. Karenanya, upaya penjagaan data pribadi konsumen diharuskan sebagai keutamaan penting setiap penyedia layanan demi menjaga kepercayaan publik dan integritas perusahaan di tengah transformasi digital yang semakin kompleks.

Terdapat sanksi administratif jika terjadinya kebocoran data pribadi menurut, Pasal 57 Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi kebijakan mengenai sanksi administratif untuk pelanggar aturan perlindungan data pribadi. Hal tersebut meliputi peringatan tertulis, pemberhentian sesaat aktivitas progres data pribadi, menghapus ataupun memusnahkan data pribadi, serta denda administratif. Besaran denda administratif bisa mencapai tertinggi 2% berdasar gaji maupun penghasilan tahunan terkait variabel konsumen yang dilakukan. Penjatuhan sanksi ini dilaksanakan pihak berwenang berdasar peraturan perundang-undangan dan mekanisme prosedur pemberian sanksi lebih lanjut dijelaskan dalam Peraturan Pemerintah. Selain sanksi administratif, pelanggaran yang bersifat serius mampu berakhir pada pidana dengan ancaman hukuman penjara hingga 6 tahun dan/atau denda maksimal Rp6 miliar. Ketentuan ini bertujuan memberikan efek jera bagi pelanggar yang sengaja melakukan penyalahgunaan data demi keuntungan pribadi atau pihak lain, sekaligus memastikan penjagaan kokoh bagi hak serta keamanan data pribadi masyarakat Indonesia (Di et al., 2023).

Perlindungan Data Pribadi Pelanggan dalam Perspektif UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

Perlindungan data pribadi pelanggan merupakan peristiwa kritis di kompleksnya era digital. Peningkatan teknologi informasi serta komunikasi membuat transformai kegiatan warga memperoleh fasilitas, bertransaksi, serta berinteraksi, baik dalam sektor publik maupun swasta. Akibatnya, data pribadi menjadi aset penting yang banyak dikumpulkan, disimpan, dan diproses oleh berbagai penyelenggara sistem elektronik, termasuk oleh perusahaan teknologi, perbankan, layanan *e-commerce*, asuransi, hingga penyedia layanan digital lainnya. Pada hal ini, data pribadi konsumen sangat rentan terhadap risiko penyalahgunaan, kebocoran, pencurian data, hingga praktik perdagangan data ilegal. Karenanya, adanya Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi (UU PDP) menjadi suatu langkah monumental dalam memberikan dasar hukum yang kuat terhadap perlindungan hak mengenai kerahasiaan serta data pribadi tiap individu, termasuk konsumen.

Selain itu, UU PDP mendefinisikan data pribadi secara komprehensif, sebagaimana tercantum dalam Pasal 1 angka 1, yakni setiap data tentang seseorang yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri maupu dikolaborasikan melalui fakta lain, dengan langsung atau tak langsung, dengan tatanan elektronik maupun non-elektronik. Paparan ini menegaskan bahwa data pribadi tidak hanya terbatas di informasi yang eksplisit seperti nama, alamat, dan nomor induk kependudukan (NIK), tetapi juga mencakup data yang lebih rentan, berupa biometrik, kesehatan, finansial, hingga rekam jejak elektronik. UU PDP bahkan memisahkan data pribadi dalam dua kategori besar, yakni pribadi biasa serta pribadi rinci (sensitif), di mana perlindungan terhadap data spesifik dilakukan secara lebih ketat karena memiliki potensi risiko yang lebih besar bila disalahgunakan.

Berdasarkan pemikiran Philipus M. Hadjon sebagaimana disebut dalam teori ini menekankan kewajiban negara dan pelaku usaha untuk memberikan perlindungan preventif dan represif terhadap HAM, mencakup hak data pribadi. Teori tersebut akan digunakan untuk mengevaluasi efektivitas ketentuan sanksi dan mekanisme penegakan hukum dalam Undang-Undang PDP terhadap praktik penyebaran data yang dilakukan secara illegal (Hansen Samin, 2023).

Mengenai hak-hak subjek data pribadi dijelaskan pada Pasal 5 s.d. Pasal 15 UU PDP diantaranya, terutama hak mendapat informasi berupa identitas, dasar hukum, tujuan dimintanya serta pemakaian data juga tanggung jawab pemohon atas data pribadi tersebut, hak untuk menghentikan pengolahan, penghapusan dan/atau pemusnahan data pribadi. perlindungan data pribadi mengenai dirinya, serta hak guna penuntutannya juga mendapatkan kompensasi dari agresi data pribadi (Usman and Satria).

Upaya preventif dalam PDP adalah langkah-langkah yang dilakukan untuk mencegah terjadi pelanggaran atau kebocoran data sejak awal. Contohnya adalah memastikan data dikumpulkan secara sah, menggunakan enkripsi, membatasi akses data, menjalankan pelatihan kesadaran keamanan, membuat kebijakan perlindungan data, dan edukasi literasi digital. Tujuannya agar data pribadi dikelola dengan aman dan transparan sehingga tidak merugikan pemilik data (Widigdo & Ferry Rosando, 2023).

Upaya represif dalam PDP adalah tindakan yang diambil setelah terjadi pelanggaran data, untuk menangani masalah tersebut dan memberikan sanksi kepada pelanggar. Ini meliputi pengusutan pelanggaran, pemberian hukuman administratif atau pidana sesuai peraturan seperti UU PDP, dan solusi masalah dengan litigasi atau non-litigasi. Tujuan represif adalah memberi efek jera agar pelanggaran serupa tidak terulang dan melindungi korban pelanggaran.

UU PDP bertujuan untuk menjaga hak konstitusional subjek data pribadi dengan cara mengatur tata kelola data pribadi supaya diproses secara sah, transparan, dan bertanggung jawab. Prinsip-prinsip dasar dalam UU ini meliputi legalitas pemrosesan, tujuan yang jelas, relevansi data yang dikumpulkan, serta jangka waktu retensi dan pemrosesan data yang dibatasi. UU ini juga menegaskan hak subjek data (dalam hal ini, konsumen) guna mengawasi data pribadinya, juga hak pengaksesan, perbaikan, penghapusan, serta pembatasan pemakaian data pribadi.

Pelanggan berhak mendapatkan kejelasan informasi mengenai siapa yang mengelola data mereka, untuk tujuan apa data tersebut digunakan, dan jangka waktu pemakaiannya. Mereka juga berhak untuk memperbaiki data yang kurang akurat, mengajukan penghapusan, serta mendapatkan perlindungan dari penyalahgunaan data. Mekanisme pengaduan dan kompensasi juga dijamin jika terjadi pelanggaran atas hak-hak konsumen tersebut.

Pada perkembangan teknologi digital pesat, data pribadi konsumen merupakan aset yang begitu rawan pada kebocoran dan penyelewengan. UU PDP memberi landasan hukum yang kokoh guna menjamin keamanan, privasi, serta hak-hak pelanggan dalam dunia digital, sekaligus mendukung terciptanya iklim bisnis digital yang terpercaya dan bertanggung jawab di Indonesia.

Tujuan penting perlindungan data pribadi menurut Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi (UU PDP) adalah memberi perlindungan yang memadai bagi tiap seseorang supaya data pribadi mereka tak diselewengkan, diakses, atau diungkapkan tanpa izin. UU ini menegaskan hak subjek data untuk mengendalikan informasi yang berkaitan dengan dirinya, termasuk hak untuk mengetahui, memperbaiki, membatasi penggunaan, serta menghapus data pribadi tersebut jika diperlukan. Dengan demikian, UU PDP bertujuan menjaga privasi individu sekaligus memastikan transparansi dan akuntabilitas dalam pengelolaan data oleh banyak pihak, termasuk pemerintah atau swasta.

Disamping itu, UU PDP memberikan rancangan hukum yang jelas untuk pengaturan tata kelola data pribadi supaya data tersebut diproses secara etis, aman, dan bertanggung jawab. Hal tersebut krusial guna pencegahan risiko kebocoran dan penyelewengan serta membuat rugi

konsumen serta masyarakat luas. Perlindungan data tidak hanya berfokus pada keamanan teknis, tetapi juga aspek hukum dan etika yang mendasari penggunaan data pribadi sebagai amanah yang harus dijaga oleh pengendali dan prosesor data.

Lebih jauh, tujuan lain dari perlindungan data pribadi adalah membangun dan mempertahankan kepercayaan masyarakat terhadap layanan digital dan ekonomi digital secara luas. Dengan adanya perlindungan yang kuat, konsumen merasa lebih nyaman menggunakan layanan digital tanpa khawatir akan risiko penyalahgunaan data, sehingga dapat mendorong pertumbuhan bisnis yang sehat dan berkelanjutan. Maka dari itu, penerapan UU PDP juga mendukung perkembangan teknologi digital yang bertanggung jawab serta memperkuat tata kelola data pribadi sesuai standar internasional.

Terakhir, UU PDP juga mengarah pada penegakan hukum yang efektif melalui pemberian sanksi administratif dan sanksi pidana bagi pihak yang melanggar ketentuan perlindungan data pribadi, yang dimaksudkan agar ada dampak jera bagi pelaku pelanggaran serta memastikan hak-hak konsumen benar-benar terlindungi secara menyeluruh. Dengan mekanisme pengawasan dan penegakan hukum yang jelas, penjagaan data pribadi tak cuma menjadi kewajiban formal, namun pun diwujudkan dalam tindakan nyata guna menjaga keamanan dan hak konstitusional setiap individu.

Pasal 13 ayat dua (2) mengatur bahwa Subjek Data Pribadi memiliki hak memakai serta mengirim Data Pribadi mengenai mereka pada Pengelola Data Pribadi lain, selama tatanan yang dipakai mampu berkomunikasi dengan aman dan tetap mengikuti kaidah pelindungan data pribadi sesuai dengan undang-undang ini. Dengan demikian, subjek data mempunyai hak untuk memindahkan data pribadinya antar penyelenggara sistem elektronik, misalnya dalam konteks perpindahan layanan atau migrasi data, asalkan proses tersebut dilakukan melalui sistem yang terjamin keamanannya dan mematuhi ketentuan perlindungan data yang berlaku.

Pasal 12 Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi mengatur jika Subjek Data Pribadi memiliki hak untuk menuntut serta mendapat ganti rugi dari penyelewengan pengolahan data pribadi yang terjadi pada mereka selaras aturan perundang-undangan. Ketentuan ini memberikan jaminan hukum bahwa setiap individu yang mengalami kerugian akibat penyalahgunaan, kebocoran, atau pemrosesan data pribadi secara tidak sah dapat menuntut pertanggungjawaban dari pihak pengendali data pribadi atau pihak lain yang bertanggung jawab.

Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi memberi pijakan hukum yang sangat penting guna menjaga data pribadi konsumen di era digital saat ini. Dengan hadirnya regulasi ini, diharapkan hak-hak subjek data dapat terpenuhi secara optimal melalui pengelolaan data yang transparan, akuntabel, dan bertanggung jawab oleh para pengendali dan prosesor data. UU PDP tidak hanya menekankan pada aspek teknis keamanan data, tetapi juga menegaskan perlunya perlindungan hukum yang kuat, termasuk hak untuk mengakses, memperbaiki, menghapus data, serta mendapatkan ganti rugi apabila hak tersebut dilanggar.

Lebih jauh, UU PDP turut membangun fondasi kepercayaan antara konsumen dan pelaku usaha digital, sehingga dapat mendorong pertumbuhan ekonomi digital yang kontinu serta menyeluruh. Regulasi ini mendorong terciptanya iklim bisnis yang sehat dan bertanggung jawab dengan memastikan bahwa data pribadi konsumen tidak menjadi barang yang mudah disalahgunakan atau diperdagangkan secara ilegal. Selain itu, mekanisme pengawasan dan sanksi tegas yang diatur pada undang-undang pun memberi dampak jera untuk berbagai pihak pelanggar ketentuan perlindungan data.

Dengan perkembangan teknologi informasi yang terus meningkat, perlindungan data pribadi menjadi aspek strategis yang tidak bisa diabaikan. Oleh karena itu, implementasi UU PDP memerlukan sinergi yang kuat dari seluruh pihak, dari pemerintah, pelaku usaha, sampai konsumen sendiri, guna menumbuhkan wawasan serta kognisi mengenai pentingnya menjaga privasi dan keamanan data pribadi. Kesadaran ini penting agar perlindungan data tidak hanya menjadi formalitas hukum, melainkan menjadi budaya dan kewajiban bersama dalam menghadapi tantangan dunia digital.

D. Kesimpulan

Tanggung jawab provider dalam melindungi data pribadi konsumen diatur secara tegas oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang mengharuskan penyelenggara layanan menjaga keamanan, kerahasiaan, dan integritas data agar terhindar dari kebocoran dan penyalahgunaan. Prinsip *strict liability* menegaskan tanggung jawab penuh *provider*, termasuk atas tindakan pihak ketiga, sehingga standar pengamanan ketat serta transparansi menjadi kunci. UU PDP juga memberikan hak-hak konsumen untuk mengakses, memperbaiki, dan menghapus data pribadi, serta menyediakan mekanisme pengaduan dan kompensasi jika terjadi pelanggaran, disertai sanksi administratif dan pidana untuk efek jera.

Perlindungan data pribadi konsumen yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 menjadi landasan hukum penting di era digital untuk menjaga keamanan, privasi, dan hak-hak konsumen dari penyalahgunaan serta kebocoran data. UU ini memberi definisi yang komprehensif tentang data pribadi, mengatur hak subjek data untuk mengakses, memperbaiki, dan menghapus data mereka, serta mewajibkan pengendali data untuk memproses data secara transparan dan bertanggung jawab.

Saran

Provider harus meningkatkan standar keamanan data dengan menerapkan teknologi enkripsi dan sistem pengamanan yang mutakhir untuk mencegah kebocoran dan penyalahgunaan data pribadi konsumen. Selain itu, penting bagi provider untuk melakukan pengawasan ketat terhadap mitra kerja yang memiliki akses data serta mengikat mereka dengan perjanjian Non-*Disclosure Agreement (NDA)* guna meminimalisir risiko kebocoran yang disebabkan oleh kelalaian atau tindakan oknum.

Pelindungan Data Pribadi harus dilakukan oleh seluruh pihak, terutama pelaku usaha, untuk menjamin pengelolaan data yang aman, transparan, dan bertanggung jawab. Pemerintah perlu terus menguatkan pengawasan dan penegakan hukum agar perlindungan data benar-benar efektif dan memberikan efek jera bagi pelanggar.

E. Referensi

Tehupeiory, A., (2021)_. *Bahan Ajar Metode Penelitian Hukum*. Jakarta: UKI Press.

ADY, Malhan, T., Budi. A. D. P., (2023). Tinjauan Yuridis Terhadap Perlindungan Konsumen Atas Penyedia Jasa Layanan Pinjaman Berbasis Teknologi Informasi. Kajian Hukum, , 8.1: 35-49.

Di, Anak, Bawah Umur, Di Indonesia, Serta Perbandingan, Regulasi Anak, Di Bawah, Umur Di, et al. 2023. "Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa (General Data Protection Regulation)." *Lex Patrimonium* 2(2): 12. https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/12.

Samin, H., Herol. (2023). "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif." *Jurnal Sains Student Research* 1(2): 1–15. https://doi.org/10.61722/jssr.v1i3.386.

Hufron. (2022). *KONSEP PENGATURAN KEWENANGAN & PERTANGGUNGJAWABAN WAKIL PRESIDEN INDONESIA*. ed. R Ari Nugroho. Yogyakarta: Jejak Pustaka.

Pranindya, K. R. A., (2025). "Penegakan Hukum Terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Melalui Barcode Ditinjau Dari UU ITE Dan UU Nomor 27 Tahun 2022 Tentang (UU PDP)." *Konsensus : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 2(3): 123–35. doi:10.62383/konsensus.v2i3.957.

Kusnadi, Ayumeida, S., (2021). "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2(1): 9–16. doi:10.47776/alwasath.v2i1.127.

Mahameru, Erlangga,D., Nurhalizah, A., Wildan, A., Badjeber, M. H., & Rahmadia, M. H., (2023). "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Jurnal Esensi Hukum* 5(2): 115–31. https://journal.upnvj.ac.id/index.php/esensihukum/index.

Nafi'ah, Rahmawati. (2020). "Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce." *Cyber Security dan Forensik Digital* 3(1): 7–13. doi:10.14421/csecurity.2020.3.1.1980.

Jalaludin, R., Ady, P., Mardina, R., Muksalmina, Muhammad, R. T., Nasruddin, H. K., Ibnu., (2023). *Metodologi Penelitian Hukum*. ed. Iftitah Anik. Sada Kurnia Pustaka.

Usman, bin, B., & Satria, U. P. E., (2024). "Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP Legal." *Doktrina Journal of Law* 7(27): 178–201.

Vania., Cindy., Markoni., Saragih, H & Widarto, J., (2023). "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber." *Jurnal Multidisiplin Indonesia* 2(3): 654–66. doi:10.58344/jmi.v2i3.157.

Widigdo, Zefaki, & Rosando, A. F., (2023). "Perlindungan Negara Terhadap Privasi Data Pribadi Dalam Layanan Sim Card Di Era Digital." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3(1): 679–96. doi:10.53363/bureau.v3i1.210.

Wiryany, Detya, Natasha, S., Kurniawan, R., (22022). Jurusan Ilmu Komunikasi, and Membangun Bandung.. 8 Jurnal Nomosleca, Oktober *PERKEMBANGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI TERHADAP PERUBAHAN SISTEM KOMUNIKASI INDONESIA*.