Pelindungan Hukum Terhadap Data Pribadi Di Indonesia

Abdul Rauf[1*], Annah[2], Hardi[1], Mudarsep[1]
[1]Jurusan Sistem Informasi, [2]Rekayasa Perangkat Lunak Universitas Dipa Makassar
Jl. Perintis Kemerdekaan Km.9 Makassar Telp. (0411) 587194
e-mail: [*1]abdul_rauf@undipa.ac.id

Abstrak

Transformasi digital dalam era telematika membawa dampak besar terhadap pola interaksi sosial dan ekonomi. Namun, perkembangan ini juga menghadirkan tantangan serius dalam pelindungan data pribadi. Indonesia sebagai negara berkembang menghadapi dilema antara kebutuhan akan digitalisasi dan urgensi pelindungan hak privasi warga Negara, sehingga permasalahan yang muncul adalah bagaimana pengaturan tentang pelindungan data pribadi di Indonesia sesuai dengan ketentuan hukum yang berlaku. Berdasarkan permasalahan tersebut, maka dalam penelitian ini akan dianalisis mengenai pelindungan data pribadi di Indonesia dan penyelesaian hukumnya jika terjadi pelanggaran, termasuk bagaimana tantangan yuridis yang akan dihadapi serta solusi normatif yang ditawarkan sesuai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Hasil penelitian menunjukkan bahwa secara normatif data pribadi terdiri atas dua macam yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Untuk memperkuat upaya pelindungan terhadap data pribadi perlu dibentuk lembaga pengawas. Penyelesaian sengketa terkait pelindungan data pribadi dapat dilakukan melalui jalur pengadilan (litigasi) maupun non litigasi atau alternative dispute resolution (ADR) melalui arbitrase atau medasi.

Kata kunci: *Pelindungan, Hukum, Data Pribadi, Online.*

Abstract

Digital transformation in the telematics era has a major impact on social and economic interaction patterns. However, this development also presents serious challenges in protecting personal data. Indonesia as a developing country faces a dilemma between the need for digitalization and the urgency of protecting citizens' privacy rights, so the problem that arises is how to regulate the protection of personal data in Indonesia in accordance with applicable legal provisions. Based on these problems, this study will analyze the protection of personal data in Indonesia and its legal resolution if a violation occurs, including the legal challenges that will be faced and the normative solutions offered in accordance with Law Number 27 of 2022 concerning Protection of Personal Data. The results of the study show that normatively personal data consists of two types, namely specific personal data and general personal data. To strengthen efforts to protect personal data, a supervisory institution needs to be formed. Settlement of disputes related to the protection of personal data can be done through the courts (litigation) or non-litigation or alternative dispute resolution (ADR) through arbitration or mediation.

Keywords*: Protection, Law, Personal Data, Online.*

1. PENDAHULUAN

Pesatnya kemajuan teknologi informasi dan komunikasi membawa banyak peluang, tapi juga tantangan tersendiri. Teknologi ini memungkinkan orang-orang di seluruh dunia untuk saling terhubung tanpa batas wilayah negara, dan hal ini menjadi salah satu penggerak utama globalisasi. Hampir semua bidang kehidupan kini memanfaatkan teknologi informasi mulai dari perdagangan lewat e-commerce, pembelajaran melalui e-education, layanan kesehatan digital atau e-health, hingga layanan publik yang dijalankan lewat sistem e-government. Semua ini menunjukkan bahwa perkembangan teknologi informasi dan komunikasi telah mengubah cara dunia bekerja, termasuk dalam ranah hukum secara global.

Meningkatnya penggunaan platform digital dalam berbagai aktivitas seperti transaksi, layanan publik, dan interaksi sosial turut memperbesar potensi risiko terjadinya kebocoran, penyalahgunaan, hingga perdagangan data pribadi. Kondisi ini menegaskan urgensi perlunya sistem pelindungan hukum yang kuat dan mampu beradaptasi dengan perkembangan teknologi. Salah satu contoh pelanggaran terhadap pelindungan data pribadi yang telah melalui proses peradilan adalah Perkara No. 77/Pid.Sus/2024/PN Tng

dan Perkara No. 78/Pid.Sus/2024/PN Tng. Dalam kedua perkara tersebut, data pribadi milik orang lain disalahgunakan untuk registrasi kartu perdana, yang kemudian dijual demi memperoleh keuntungan finansial [1].

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan amanat dari Pasal 28G ayat (1) UndangUndang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa, "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Ketentuan ini kemudian menjadi dasar lahirnya undang-undang tentang pelindungan data pribadi.

Permasalahan terkait pelindungan data pribadi pada dasarnya berangkat dari keprihatinan atas potensi pelanggaran yang dapat dialami oleh setiap individu maupun badan hukum. Pelanggaran terhadap data pribadi ini dapat berdampak serius, baik secara materiel maupun nonmateriel. Oleh karena itu, pelindungan data pribadi bertujuan untuk menjamin dan melindungi hak-hak individu dalam masyarakat, khususnya yang berkaitan dengan proses pengolahan data pribadi, baik melalui sistem elektronik maupun non-elektronik.

Pelindungan yang memadai terhadap data pribadi akan membangun kepercayaan publik untuk memberikan data mereka guna berbagai keperluan, tanpa khawatir akan penyalahgunaan atau pelanggaran atas hak pribadinya. Dengan adanya pengaturan yang jelas, diharapkan tercipta keseimbangan antara perlindungan hak individu dan kepentingan masyarakat yang diwakili oleh negara. Aturan mengenai pelindungan data pribadi juga berperan penting dalam mendukung ketertiban dan kemajuan masyarakat di era informasi. Meski demikian, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi masih bersifat umum, sehingga setiap sektor diharapkan dapat mengadaptasikan pelindungan data pribadi sesuai dengan kebutuhan dan karakteristik masing-masing bidang.

Tujuan dari pengaturan pelindungan data pribadi antara lain adalah untuk melindungi dan menjamin hak-hak dasar setiap warga negara, khususnya yang berkaitan dengan perlindungan atas privasi individu. Selain itu, regulasi ini juga memastikan agar masyarakat dapat memperoleh layanan yang layak dari korporasi, lembaga publik, organisasi internasional, maupun pemerintah. Di sisi lain, pengaturan ini diharapkan mampu mendorong pertumbuhan ekonomi digital serta perkembangan industri teknologi informasi dan komunikasi, sekaligus memperkuat daya saing industri dalam negeri.

Pelindungan data pribadi merupakan bagian dari pelindungan hak asasi manusia, sehingga pengaturannya mencerminkan pengakuan dan penghormatan terhadap hak-hak dasar setiap individu. Oleh karena itu, keberadaan Undang-Undang yang mengatur pelindungan data pribadi menjadi hal yang sangat penting dan tidak dapat diabaikan, mengingat urgensinya bagi kepentingan nasional. Selain itu, keterlibatan Indonesia dalam hubungan internasional juga menuntut adanya sistem pelindungan data pribadi yang memadai. Kehadiran regulasi tersebut dapat mendukung kelancaran aktivitas perdagangan, industri, dan investasi lintas negara.

Pelindungan data pribadi berlandaskan pada hak atas privasi, yang merupakan bagian dari Hak Asasi Manusia (HAM). Alan Westin mendefinisikan privasi sebagai hak individu untuk mengendalikan informasi pribadinya serta membatasi siapa saja yang dapat mengaksesnya[2]. Dalam perspektif hukum, privasi tidak hanya dimaknai sebagai kebebasan dari gangguan, tetapi juga sebagai pengakuan atas hak individu untuk memiliki kendali atas data pribadinya. Secara filosofis, pelindungan hukum terhadap data pribadi didasari oleh beberapa prinsip, salah satunya adalah konsep hak asasi manusia. Dalam konteks ini, setiap individu diakui memiliki hak atas privasi dan kendali terhadap informasi pribadi sebagai bagian dari harkat dan martabat manusia serta kebebasan individu. Meskipun UUD Negara Republik Indonesia Tahun 1945 tidak secara tegas menyebutkan hak atas data pribadi, namun jaminan terhadap privasi termuat dalam Pasal 28G ayat (1), yang menyatakan bahwa "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta bendanya serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Pasal ini, jika ditafsirkan secara luas, mencakup pula pelindungan atas informasi pribadi sebagai bagian dari pelindungan terhadap kehormatan dan identitas pribadi seseorang.

Kedua, prinsip kedaulatan informasi menegaskan bahwa setiap individu berhak untuk mengatur bagaimana data pribadinya dikumpulkan, digunakan, maupun dibagikan. Prinsip ini menempatkan individu sebagai pemilik dan pengendali utama atas informasi pribadinya. Oleh karena itu, diperlukan adanya persetujuan yang jelas dan berdasarkan pemahaman yang memadai (informed consent) dari pemilik data sebelum proses pengolahan data dilakukan.

Ketiga, prinsip keadilan dan keseimbangan kekuasaan menjadi penting dalam hubungan antara individu sebagai pemilik data dengan institusi, organisasi, atau perusahaan yang mengelola dan memproses data dalam jumlah besar. Regulasi pelindungan data pribadi berperan untuk menjaga keseimbangan tersebut, mencegah potensi penyalahgunaan informasi, serta memastikan bahwa pihak yang mengendalikan data bertanggung jawab atas setiap tindakan yang dilakukan terhadap data tersebut.

Dalam konteks ekonomi global, pelindungan data pribadi telah menjadi salah satu instrumen penting dalam mendukung kelancaran perdagangan internasional. Jaminan atas pelindungan data menjadi syarat yang dibutuhkan oleh berbagai mitra kerja sama ekonomi internasional, seperti Organisation for Economic Cooperation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), dan Economic Community of West African States (ECOWAS). Bahkan, organisasi-organisasi tersebut telah membentuk instrumen khusus untuk memastikan perlindungan data pribadi dalam setiap transaksi lintas negara. Sebagai negara dengan posisi strategis dalam perdagangan internasional, Indonesia memiliki kepentingan besar untuk menyusun regulasi pelindungan data pribadi yang memadai dan sesuai dengan standar global. Namun, jika dibandingkan dengan negara-negara ASEAN lainnya, Indonesia masih tergolong tertinggal dalam hal kesiapan regulasi dan sistem pelindungan data pribadi, baik dari segi waktu implementasi maupun cakupan perlindungannya [3].

Pemahaman mengenai pelindungan data pribadi tidak dapat dilepaskan dari penafsiran terhadap istilah "data" yang dikategorikan sebagai "data pribadi", serta bagaimana mekanisme pelindungan yang seharusnya diberikan terhadap data tersebut. Secara etimologis, kata data merupakan bentuk jamak dari datum, yang dalam bahasa Latin berarti bagian dari informasi [4]. Dengan demikian, data dapat dipahami sebagai kumpulan datum yang membentuk suatu informasi. Data juga harus memuat serangkaian fakta dalam bentuk simbol, seperti huruf, angka, gambar, atau tanda-tanda khusus lainnya yang merepresentasikan ide, objek, keadaan, atau situasi tertentu, dan dapat disusun untuk diproses dalam bentuk struktur data, struktur file, maupun basis data [5]. Seiring berkembangnya metode pengumpulan data, berbagai jenis dan klasifikasi data pun muncul, seperti data primer dan sekunder, data kualitatif dan kuantitatif, hingga data pribadi yang menjadi perhatian utama dalam pelindungan hak individu di era digital saat ini.

Dalam konteks data pribadi, saat ini berbagai negara di dunia menggunakan istilah yang berbeda untuk merujuk pada konsep serupa, yaitu antara "informasi pribadi" dan "data pribadi." Meskipun berbeda secara terminologi, keduanya memiliki makna yang hampir identik dan sering digunakan secara bergantian. Negara-negara seperti Amerika Serikat, Kanada, dan Australia umumnya menggunakan istilah personally identifiable information (PII) atau informasi pribadi, sementara negara-negara di kawasan Eropa dan juga Indonesia lebih sering menggunakan istilah personal data atau data pribadi. Oleh karena itu, dalam pembahasan ini, penulis memilih menggunakan istilah "data pribadi" sebagai acuan. Lebih jauh lagi, perbedaan tidak hanya terletak pada istilah yang digunakan, tetapi juga pada cara penafsiran terhadap istilah tersebut. Sistem hukum di Amerika Serikat, misalnya, tidak memiliki instrumen hukum tunggal yang secara tegas mendefinisikan data pribadi. Sebaliknya, mereka menggunakan tiga pendekatan dalam memahami istilah tersebut, yaitu pendekatan tautologis (tautological approach), pendekatan berdasarkan informasi non-publik (non-public approach), dan pendekatan berbasis jenis data tertentu (specific type approach) [6].

Dalam upaya melindungi data pribadi, terdapat dua pendekatan utama yang umum dikenal. Pertama, pelindungan dilakukan melalui pengamanan fisik terhadap data pribadi itu sendiri, misalnya dengan penggunaan kata sandi (password) atau sistem keamanan teknis lainnya. Pendekatan ini bersifat preventif dan teknologis guna mencegah akses tidak sah. Kedua, pelindungan dilakukan melalui mekanisme hukum berdasarkan peraturan perundang-undangan yang berlaku, dengan tujuan untuk memberikan kepastian hukum dan menjamin hak atas privasi individu terkait penggunaan data pribadinya. Berkaitan dengan pendekatan kedua ini, sejarah mencatat bahwa konsep pelindungan data pribadi yang dikenal dengan istilah data protection pertama kali diatur dalam undang-undang di sejumlah negara Eropa seperti Jerman, Swedia, dan Prancis pada era 1970-an. Regulasi di negara-negara tersebut lahir dari kesadaran akan pentingnya menjamin hak individu atas privasi dalam era modern yang semakin bergantung pada pengelolaan data [7].

Konsep pelindungan data kerap dianggap sebagai bagian integral dari pelindungan hak atas privasi. Pada dasarnya, pelindungan data memiliki keterkaitan yang erat dengan privasi, sebagaimana dijelaskan oleh Alan Westin yang merupakan salah satu tokoh pertama yang mendefinisikan konsep information privacy. Menurut Westin, privasi informasi merupakan hak individu, kelompok, atau institusi untuk mengatur sendiri kapan, bagaimana, dan sejauh mana informasi tentang diri mereka dapat diungkapkan atau dibagikan kepada pihak lain [8].

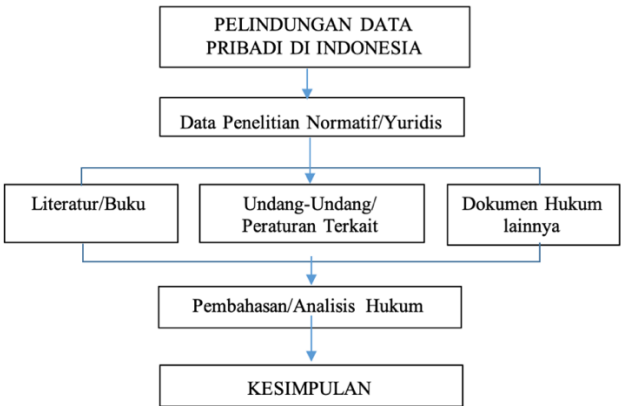
Meskipun Indonesia telah memberlakukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, masih terdapat banyak pihak khususnya pelaku usaha yang belum sepenuhnya memahami tanggung jawab hukum yang melekat pada mereka. Kurangnya pemahaman ini berdampak pada rendahnya tingkat kepatuhan terhadap prinsip-prinsip pemrosesan data pribadi. Selain itu, Indonesia juga kerap menghadapi kasus kebocoran data yang melibatkan sejumlah lembaga, yang kemudian menimbulkan berbagai persoalan hukum, seperti pertanggungjawaban langsung dari pihak pengendali data, kejelasan sanksi yang dapat dikenakan, serta mekanisme penyelesaian sengketa apabila terjadi pelanggaran terhadap data pribadi.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk mengkaji pelaksanaan pelindungan data pribadi di Indonesia serta mekanisme penyelesaiannya dari perspektif hukum, termasuk bentuk sanksi yang dapat dikenakan apabila terjadi pelanggaran. Penelitian ini juga akan membahas kerangka regulasi yang mengatur pelindungan data pribadi di Indonesia, sekaligus mengidentifikasi berbagai tantangan yang muncul dalam proses implementasinya.

Penelitian ini diharapkan dapat memberikan kontribusi baik secara akademis maupun praktis dalam memahami isu-isu pelindungan data pribadi dalam kerangka hukum yang berlaku di Indonesia. Dari aspek akademis, penelitian ini dapat dijadikan sebagai referensi dalam pengembangan teori hukum yang berkaitan dengan regulasi dan pelindungan data pribadi. Sementara dari sisi praktis, temuan dalam penelitian ini diharapkan mampu memberikan rekomendasi kebijakan yang relevan bagi pemerintah serta penyedia layanan internet (Internet Service Provider), khususnya dalam merespons berbagai tantangan yang muncul dalam upaya pelindungan data pribadi di era digital.

2. METODE PENELITIAN

Penelitian ini menerapkan metode yuridis-normatif dengan menggunakan pendekatan peraturan perundang-undangan dan pendekatan konseptual. Data dikumpulkan melalui studi kepustakaan yang mencakup regulasi nasional, dokumen hukum internasional, serta literatur akademik yang relevan dengan isu pelindungan data pribadi. Selanjutnya, analisis dilakukan secara kualitatif guna mengevaluasi kesesuaian antara norma hukum yang berlaku dengan implementasi praktik hukum dalam pelindungan data pribadi di Indonesia.



Gambar 1. Bagan Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Kerangka Hukum Pelindungan Data Pribadi di Indonesia

Kerangka hukum pelindungan data pribadi di Indonesia mengalami perkembangan yang signifikan dalam beberapa tahun terakhir. Sebelum disahkannya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), beberapa peraturan sektoral telah mengatur aspek-aspek tertentu terkait data pribadi, antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Jo UU No.19 Tahun 2016 Jo UU No. 1 Tahun 2024 tentang Perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. UU ITE mengatur tentang informasi elektronik dan transaksi elektronik, termasuk ketentuan mengenai pelindungan data pribadi dalam konteks sistem elektronik. Pasal 26 UU ITE mengatur tentang hak atas privasi dan penghapusan informasi elektronik yang tidak relevan.
2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE): PP PSTE memberikan detail lebih lanjut mengenai pengelolaan data pribadi dalam sistem elektronik, termasuk kewajiban pengamanan data dan pemberitahuan kebocoran data.
3. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik: Permenkominfo ini secara lebih spesifik mengatur prinsip-prinsip pelindungan data pribadi dalam konteks sistem elektronik, termasuk persetujuan, pembatasan tujuan, kerahasiaan, dan hak pemilik data.

4. Peraturan Bank Indonesia (PBI) dan peraturan sektoral lainnya: Beberapa sektor seperti perbankan dan telekomunikasi juga memiliki peraturan yang mengatur pelindungan data pribadi konsumen dalam lingkup industri masing-masing.

3.2. UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

Disahkannya Undang-Undang Pelindungan Data Pribadi (UU PDP) merupakan langkah penting dalam perkembangan sistem hukum yang mengatur pelindungan data pribadi di Indonesia. Undang-undang ini secara menyeluruh mencakup berbagai aspek penting, termasuk definisi data pribadi, prinsip-prinsip dalam pemrosesan data, hak-hak subjek data, kewajiban yang harus dipenuhi oleh pengendali dan pemroses data, serta mekanisme penegakan hukum yang dapat ditempuh apabila terjadi pelanggaran.

Beberapa prinsip utama yang diatur dalam UU PDP meliputi:

1. Persetujuan (Consent): Pemrosesan data pribadi harus didasarkan pada persetujuan eksplisit dari subjek data, kecuali dalam kondisi tertentu yang diizinkan oleh undang-undang.
2. Pembatasan Tujuan: Data pribadi hanya boleh diproses sesuai dengan tujuan yang telah ditentukan dan diinformasikan kepada subjek data.
3. Minimalisasi Data: Data pribadi yang diproses harus relevan dan terbatas pada apa yang diperlukan untuk tujuan pemrosesan.
4. Kerahasiaan dan Keamanan: Pengendali data wajib menjaga kerahasiaan dan keamanan data pribadi dari akses yang tidak sah atau penyalahgunaan.
5. Akuntabilitas: Pengendali data bertanggung jawab atas kepatuhan terhadap prinsip-prinsip pelindungan data pribadi.
6. Hak Subjek Data: UU PDP memberikan sejumlah hak kepada subjek data, termasuk hak untuk mengakses, memperbaiki, menghapus, menarik persetujuan, dan mengajukan keberatan terhadap pemrosesan data pribadi mereka.

Merujuk pada ketentuan Pasal 4 ayat (1) Undang-Undang Nomor 27 Tahun 2022, data pribadi diklasifikasikan ke dalam dua kategori, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Data pribadi yang bersifat spesifik mencakup informasi sensitif seperti data dan riwayat kesehatan, data biometrik, data genetika, catatan kriminal, data anak, informasi keuangan pribadi, serta jenis data lainnya yang diatur dalam peraturan perundang-undangan. Sementara itu, data pribadi yang bersifat umum meliputi informasi seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, atau data lain yang apabila dikombinasikan dapat digunakan untuk mengidentifikasi seseorang secara langsung.

3.3. Mekanisme Pelindungan Hukum Terhadap Data Pribadi

Berdasarkan ketentuan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP), setiap subjek data pribadi memiliki hak untuk memperoleh informasi yang jelas mengenai identitas pihak yang meminta data, dasar kepentingan hukum yang melandasi permintaan tersebut, tujuan penggunaan data pribadi, serta tanggung jawab atau akuntabilitas dari pihak yang mengakses atau memproses data tersebut. Dengan demikian, setiap individu sebagai pemilik data pribadi dijamin memiliki sejumlah hak yang melekat atas data miliknya:

1. Hak atas informasi
2. Hak untuk memperbaiki/melengkapi data
3. Hak untuk menghapus/memusnahkan data
4. Hak menolak pemrosesan otomatis
5. Hak untuk menarik persetujuan
6. Hak mengajukan keberatan dan keluhan

Pelaksanaan hak-hak Subjek Data Pribadi dilakukan dengan mengajukan permohonan secara tertulis dan terdokumentasi, baik melalui media elektronik maupun non-elektronik, kepada Pengendali Data Pribadi (Data Controller). Pihak pengendali data pribadi berkewajiban:

1. Memastikan dasar hukum pemrosesan data
2. Memastikan adanya persetujuan sah
3. Melindungi data dengan sistem keamanan
4. Menyampaikan pemberitahuan kepada subjek data
5. Melaporkan pelanggaran data ke otoritas

Pemrosesan Data Pribadi dilakukan oleh Prosesor Data Pribadi (Data Processor) dengan tujuan untuk menjaga keamanan data dari akses, pengungkapan, perubahan, penyalahgunaan, perusakan, atau penghilangan yang tidak sah. Dalam menjalankan tugasnya, Prosesor Data Pribadi wajib mengikuti instruksi dari Pengendali Data Pribadi, menjamin keamanan selama proses pengolahan data berlangsung, serta tidak menggunakan data tersebut untuk kepentingan yang tidak semestinya. Adapun bentuk-bentuk pemrosesan data pribadi meliputi kegiatan seperti pengumpulan, penyimpanan, pemanfaatan, pendistribusian, hingga penghapusan data.

Berdasarkan ketentuan Pasal 20 ayat (2) UU PDP, diatur bahwa dasar hukum pemrosesan data pribadi adalah:

1. Persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi.
2. Pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian.
3. Pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.
4. Pemenuhan pelindungan kepentingan vital Subjek Data Pribadi.
5. Pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan.

Pengawasan terhadap pelaksanaan Pelindungan Data Pribadi dilakukan oleh suatu lembaga yang ditunjuk secara resmi oleh Presiden dan berada di bawah tanggung jawab langsung Presiden. Lembaga ini memiliki wewenang untuk menjalankan penegakan hukum administratif terhadap pelanggaran ketentuan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP), serta berperan dalam memfasilitasi penyelesaian sengketa di luar jalur peradilan. Kewenangan lembaga dimaksud diatur secara rinci dalam Pasal 60 UU PDP.

3.4. Sanksi dan Penyelesaian Sengketa

Jenis sanksi yang dapat dikenakan atas pelanggaran sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mencakup dua kategori, yaitu sanksi administratif dan sanksi pidana. Kedua bentuk sanksi ini diterapkan sesuai dengan tingkat pelanggaran dan ketentuan hukum yang berlaku. Jenis sanksi administratif sebagaimana yang diatur dalam Pasal 57 ayat (2) UU PDP adalah:

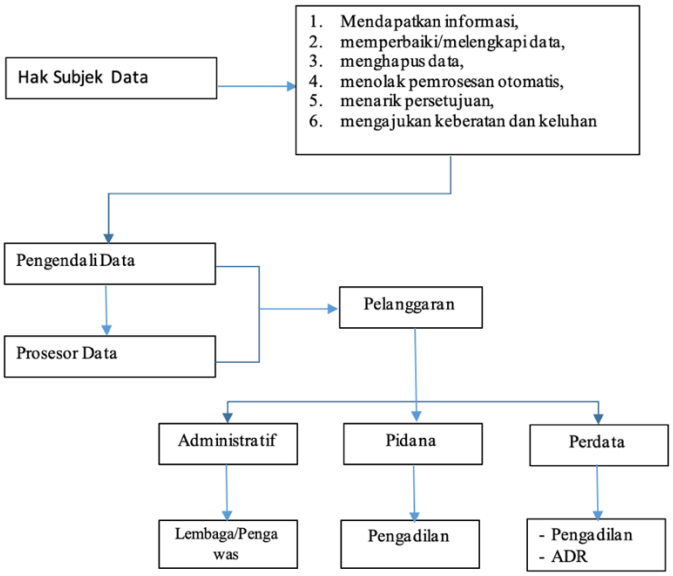
1. Peringatan tertulis.
2. Penghentian sementara kegiatan pemrosesan Data Pribadi.
3. Penghapusan atau pemusnahan Data Pribadi; dan/atau.
4. Denda administrative.

Pemberian sanksi administratif merupakan kewenangan lembaga yang ditunjuk oleh pemerintah. Adapun tata cara pelaksanaan dan mekanisme penjatuhan sanksi administratif tersebut akan diatur lebih lanjut melalui Peraturan Pemerintah sebagai peraturan pelaksana dari Undang-Undang.

Penyelesaian sengketa terkait pelindungan data pribadi dapat ditempuh melalui jalur litigasi maupun non-litigasi, antara lain melalui lembaga arbitrase atau alternatif penyelesaian sengketa lainnya, sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Proses penyelesaian sengketa dan/atau persidangan terkait pelanggaran pelindungan data pribadi mengikuti ketentuan hukum acara yang berlaku. Dalam hal pembuktian, alat bukti yang digunakan merujuk pada ketentuan hukum acara, termasuk bukti lain seperti informasi elektronik dan/atau dokumen elektronik yang sah menurut hukum.

Hal ini menunjukkan bahwa sistem penyelesaian sengketa dalam pelindungan data pribadi bersifat terbuka dan fleksibel, memberikan ruang bagi para pihak untuk memilih mekanisme penyelesaian yang paling sesuai dengan kebutuhan dan kepentingannya. Dengan pengakuan terhadap bukti elektronik sebagai alat bukti yang sah, sistem hukum Indonesia telah menyesuaikan diri dengan dinamika perkembangan teknologi informasi. Pendekatan ini tidak hanya memperkuat legitimasi proses hukum dalam ranah digital, tetapi juga mendorong kepercayaan masyarakat terhadap perlindungan hak atas data pribadi mereka melalui jalur hukum yang dapat diakses dan diandalkan.

Selain itu, keberadaan mekanisme penyelesaian sengketa yang mengakomodasi jalur non-litigasi, seperti melalui lembaga arbitrase atau alternatif penyelesaian sengketa lainnya, mencerminkan upaya untuk memberikan proses penyelesaian yang lebih cepat, efisien, dan berbiaya rendah dibandingkan proses peradilan konvensional. Hal ini menjadi penting dalam konteks pelanggaran data pribadi yang sering kali membutuhkan respons segera untuk meminimalisir dampak yang lebih luas.



Gambar 2. Mekanisme Pelindungan Hukum Data Pribadi

Berdasarkan ketentuan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP), setiap individu dilarang untuk secara melawan hukum memperoleh atau mengumpulkan data pribadi milik orang lain dengan tujuan memperoleh keuntungan pribadi maupun untuk pihak lain yang dapat menimbulkan kerugian bagi subjek data. Selain itu, tindakan mengungkapkan atau menggunakan data pribadi milik orang lain tanpa izin dan secara melawan hukum juga dilarang. Lebih lanjut, Pasal 66 UU PDP secara tegas melarang setiap orang untuk membuat atau memalsukan data pribadi dengan maksud memperoleh keuntungan pribadi atau untuk orang lain, apabila tindakan tersebut dapat merugikan pihak lain. Pelanggaran terhadap ketentuan ini merupakan tindak pidana yang dapat dikenai sanksi pidana, dan proses penanganannya mengikuti ketentuan yang berlaku dalam sistem Hukum Acara Pidana.

UU PDP merupakan pencapaian signifikan dalam membentuk ulang kerangka hukum pelindungan data pribadi di Indonesia. Meskipun demikian, proses implementasinya masih dihadapkan pada berbagai tantangan, baik dari sisi struktural maupun kultural. Di tingkat struktural, kesiapan birokrasi yang belum optimal, adanya potensi tumpang tindih kewenangan antar lembaga, serta belum terbentuknya infrastruktur yang memadai menjadi kendala utama. Sementara dari sisi kultural, kesadaran dan budaya pelindungan data di kalangan masyarakat maupun institusi masih tergolong lemah, sehingga menghambat efektivitas pelaksanaan regulasi yang telah ditetapkan.

Penerapan sanksi administratif dan pidana sebagaimana diatur dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) harus dilakukan secara konsisten agar efektif. Pasal 67 dan 68 UU PDP menetapkan ancaman pidana penjara hingga lima tahun serta denda maksimal sebesar Rp5 miliar bagi pelanggaran yang tergolong serius. Namun demikian, efektivitas penerapan sanksi tersebut sangat bergantung pada ketersediaan sistem pelaporan yang jelas serta mekanisme pembuktian yang kuat. Selain itu, ketentuan mengenai pengelolaan data sensitif—seperti data biometrik, informasi kesehatan, dan keuangan—masih memerlukan penjabaran lebih rinci melalui peraturan pelaksana. Pemerintah juga perlu menetapkan standar teknis minimum terkait keamanan sistem informasi yang wajib diterapkan oleh pengendali data, guna meminimalisasi risiko kebocoran akibat kelalaian teknis. Lebih dari itu, penguatan budaya organisasi yang menempatkan perlindungan privasi sebagai bagian dari prinsip tata kelola yang baik (good governance) menjadi hal yang krusial. Upaya preventif seperti pemberian sertifikasi pelindungan data kepada perusahaan serta pelatihan rutin bagi staf teknologi informasi dan bidang hukum dapat menjadi langkah strategis dalam mendorong kepatuhan dan meningkatkan kesadaran akan pentingnya pelindungan data pribadi.

Selain diatur dalam UU PDP, ketentuan mengenai pelindungan data pribadi juga secara umum tercantum dalam Undang-Undang Telekomunikasi, meskipun tidak secara eksplisit menyebutkan atau merinci definisi data pribadi. Salah satu ketentuan yang relevan dapat ditemukan dalam Pasal 42 ayat (1), yang menyatakan bahwa “Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang diselenggarakannya”. Berdasarkan ketentuan tersebut, penyelenggara jasa telekomunikasi memiliki kewajiban untuk menjaga kerahasiaan dan keamanan seluruh informasi yang dikirimkan atau diterima oleh pelanggan, sehingga memberikan landasan normatif terhadap perlindungan data dalam konteks layanan telekomunikasi.

UU Telekomunikasi dalam Pasal 42 Ayat (2) juga mengatur tentang pengecualian pelindungan data pribadi yaitu “Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi atas :

1. Permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu.
2. Permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-undang yang berlaku.

UU Telekomunikasi juga mengatur mengenai sanksi pidana terhadap penyalahgunaan informasi sesuai ketentuan Pasal 57 yang menyatakan bahwa “Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp.200.000.000,00 (dua ratus juta rupiah)”.

Ketentuan mengenai informasi pribadi juga tercantum dalam Undang-Undang Keterbukaan Informasi Publik (UU KIP), di mana istilah "informasi" didefinisikan secara rinci dalam Pasal 1 angka (1). Dalam ketentuan tersebut, disebutkan bahwa “Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik berupa data, fakta maupun penjelasannya, yang dapat dilihat, didengar, dan dibaca, serta disajikan dalam berbagai bentuk dan format sesuai perkembangan teknologi informasi dan komunikasi, baik secara elektronik maupun nonelektronik.” Definisi ini memberikan pemahaman yang komprehensif mengenai ruang lingkup informasi, termasuk informasi yang bersifat pribadi, dengan mempertimbangkan berbagai media penyampaiannya serta relevansinya dengan kemajuan teknologi informasi.

Informasi pada dasarnya merupakan suatu bentuk keterangan yang dapat dikemas dalam berbagai format, baik melalui media elektronik maupun non-elektronik, sejalan dengan perkembangan teknologi informasi dan komunikasi. Sementara itu, definisi mengenai informasi publik dijelaskan dalam Pasal 1 angka (2) Undang-Undang Keterbukaan Informasi Publik (UU KIP) menyatakan bahwa “Informasi Publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggaraan negara dan/atau penyelenggara badan publik lainnya, sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik”.

UU KIP juga menjelaskan beberapa jenis informasi publik yang dimaksudkan dalam Pasal 1 Angka (2). Dalam Pasal 6 Ayat (3) menyatakan bahwa : Informasi Publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah:

1. Informasi yang dapat membahayakan negara;
2. Informasi yang berkaitan dengan kepentingan pelindungan usaha dari persaingan usaha tidak sehat;
3. Informasi yang berkaitan dengan hak-hak pribadi;
4. Informasi yang berkaitan dengan rahasia jabatan; dan/atau
5. Informasi Publik yang diminta belum dikuasai atau didokumentasikan”.

Berdasarkan ketentuan Pasal 6 ayat (3) huruf (c) Undang-Undang Keterbukaan Informasi Publik, secara tersirat dapat dipahami bahwa terdapat upaya pelindungan terhadap hak-hak individu atas informasi pribadi. Informasi publik pada dasarnya kerap berkaitan dengan data diri seseorang, masyarakat, atau kelompok tertentu yang memiliki keterkaitan dengan kepentingan publik. Namun demikian, pasal tersebut menegaskan adanya batasan bahwa informasi yang berkaitan dengan hak-hak pribadi tidak dapat dibuka untuk umum. Oleh karena itu, ketentuan ini dapat dijadikan sebagai salah satu landasan normatif dalam pelindungan data pribadi, karena secara eksplisit melarang pengungkapan informasi publik yang mengandung aspek-aspek privasi individu tanpa dasar hukum yang sah.

3.5. Tantangan Hukum dalam Pelindungan Data Pribadi

Salah satu tantangan utama yang dihadapi dalam era telematika adalah rendahnya tingkat kesadaran masyarakat terhadap pentingnya pelindungan data pribadi, disertai dengan keterbatasan infrastruktur hukum yang memadai. Sebelum diberlakukannya Undang-Undang Pelindungan Data Pribadi (UU PDP), regulasi mengenai pelindungan data masih tersebar di berbagai aturan sektoral, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, serta Undang-Undang Administrasi Kependudukan [9]. Fragmentasi regulasi ini menyebabkan ketidakpastian hukum yang berpotensi melemahkan perlindungan hak individu atas datanya. Selain itu, inkonsistensi dalam penegakan hukum juga menjadi permasalahan, mengingat aparat penegak hukum masih menghadapi berbagai keterbatasan dalam menangani kejahatan siber, terutama yang bersifat lintas yurisdiksi (cross-border data flow). Keberadaan platform digital asing yang beroperasi di Indonesia tanpa kehadiran fisik juga menyulitkan proses pengawasan serta penegakan tanggung jawab hukum secara efektif.

Dari aspek kelembagaan, ketiadaan otoritas pengawas khusus yang menangani pelindungan data pribadi sebelum disahkannya UU PDP mengakibatkan lemahnya koordinasi antarinstansi serta rendahnya akuntabilitas dalam penanganan pelanggaran. Akibatnya, banyak laporan terkait pelanggaran data pribadi

yang tidak ditindaklanjuti secara optimal, karena belum tersedia standar prosedur penanganan yang bersifat nasional dan berlaku secara menyeluruh di seluruh sektor. Hal ini memperlihatkan perlunya struktur kelembagaan yang kuat dan terkoordinasi untuk menjamin perlindungan data pribadi secara efekti.

Meskipun UU PDP merupakan langkah maju yang signifikan, tantangan implementasinya tetap ada. Beberapa tantangan utama meliputi:

1. Penegakan Hukum: Efektivitas UU PDP sangat bergantung pada kemampuan aparat penegak hukum dalam mengawasi dan menindak pelanggaran data pribadi. Pembentukan lembaga pengawas pelindungan data pribadi yang independen dan berwenang menjadi krusial.
2. Kesadaran dan Literasi Data: Tingkat kesadaran masyarakat dan pemahaman mengenai hak-hak mereka terkait data pribadi masih perlu ditingkatkan. Edukasi dan sosialisasi mengenai UU PDP menjadi penting.
3. Kesiapan Organisasi: Organisasi dan perusahaan perlu melakukan penyesuaian internal untuk mematuhi ketentuan UU PDP, termasuk investasi dalam sistem keamanan data dan pelatihan sumber daya manusia.
4. Harmonisasi dengan Peraturan Sektoral: Perlu adanya harmonisasi antara UU PDP dengan peraturan sektoral yang sudah ada untuk menghindari tumpang tindih dan memastikan kepastian hukum.
5. Isu Lintas Batas: Dalam era globalisasi, transfer data pribadi lintas batas menjadi isu penting. UU PDP perlu mengakomodasi mekanisme transfer data yang aman dan sesuai dengan standar internasional.

Ke depannya, pelindungan data pribadi di Indonesia diperkirakan akan mengalami perkembangan yang semakin signifikan seiring dengan kemajuan teknologi dan meningkatnya kebutuhan masyarakat akan keamanan informasi. Undang-Undang Pelindungan Data Pribadi (UU PDP) diharapkan dapat menjadi fondasi hukum yang kokoh dalam membangun ekosistem digital yang aman, transparan, dan dapat dipercaya, di mana hak-hak individu atas data pribadi dijunjung tinggi serta dijamin perlindungannya. Untuk mendukung efektivitas implementasi regulasi ini, diperlukan penelitian dan kajian berkelanjutan terkait pelaksanaan UU PDP, efektivitas mekanisme penegakan hukum, serta kemampuan adaptasi terhadap dinamika dan inovasi teknologi. Upaya tersebut penting guna memastikan bahwa pelindungan data pribadi di Indonesia berjalan secara optimal dan responsif terhadap tantangan masa depan.

3.6. Solusi Hukum Terkait Pelindungan Data Pribadi

UU PDP yang mulai berlaku sejak 17 Oktober 2022 menjadi landasan utama dalam membangun kerangka hukum pelindungan data pribadi di Indonesia. Undang-undang ini memperkenalkan sejumlah prinsip dasar pelindungan data pribadi, antara lain legalitas, transparansi, pembatasan tujuan, akurasi, dan akuntabilitas [10]. UU PDP juga menempatkan individu sebagai subjek utama pelindungan, yang berhak mengetahui, memperbaiki, menghapus, dan menarik kembali persetujuan atas pengolahan data pribadinya. Ini merupakan pengakuan hukum atas kedaulatan data individu (data sovereignty).

Salah satu aspek penting dari UU PDP adalah pembentukan Lembaga Pelindungan Data Pribadi (LPDP), sebuah otoritas independen yang bertugas mengawasi kepatuhan pengendali dan prosesor data serta memberikan sanksi administratif [11]. Keberadaan lembaga ini penting untuk menjamin implementasi hukum secara efektif. Untuk menjawab tantangan inkonsistensi penegakan hukum, perlu dilakukan:

1. Penguatan kapasitas SDM aparat penegak hukum dalam bidang digital forensik dan regulasi data.
2. Integrasi sistem pelaporan dan pelacakan pelanggaran data pribadi.
3. Penguatan kerja sama internasional dalam hal pertukaran informasi, penyidikan lintas batas, dan harmonisasi regulasi.

Selain itu, perlu digalakkan literasi digital kepada masyarakat agar memahami hak dan kewajiban mereka sebagai subjek data. Pelaku usaha juga harus didorong untuk menerapkan "privacy by design" dalam membangun sistem digital mereka.

4. KESIMPULAN

Pelindungan data pribadi di era telematika merupakan isu strategis yang berperan penting dalam menjaga kedaulatan digital Indonesia. Undang-Undang Pelindungan Data Pribadi (UU PDP) menjadi titik awal yang krusial dalam membenahi sistem hukum nasional agar mampu merespons dinamika dan tantangan global secara adaptif. Untuk mewujudkan ekosistem digital yang aman, adil, dan bertanggung jawab, dibutuhkan komitmen yang kuat dari seluruh elemen—baik pemerintah, pelaku usaha, maupun masyarakat. Keberhasilan implementasi UU PDP sangat bergantung pada harmonisasi regulasi lintas sektor, penguatan kapasitas kelembagaan, serta transformasi budaya digital yang lebih sadar terhadap pentingnya privasi. Dalam hal penyelesaian sengketa, mekanisme hukum dapat ditempuh melalui jalur litigasi di pengadilan maupun jalur non-litigasi, seperti arbitrase atau mediasi, sesuai prinsip-prinsip penyelesaian sengketa alternatif (Alternative Dispute Resolution/ADR).

5. SARAN

Perlu adanya Lembaga Pelindungan Data Pribadi (LPDP), sebagai otoritas independen yang bertugas mengawasi kepatuhan pengendali dan prosesor data serta memberikan sanksi administratif. Selain itu perlu ada system pelaporan yang jelas bilamana terjadi pelanggaran.

DAFTAR PUSTAKA

[1] Mochamad Januar Rizki, 2025. Menelaah 3 Putusan Perkara Pelanggaran PDP, Minimnya Literasi dan Tantangannya. https://www.hukumonline.com/berita/a/ menelaah-3-putusan-perkara-pelanggaran-pdp--minimnya-literasi-dan-tantangannya-lt677bd1211839d/?page=2
[2] Alan F. Westin, Privacy and Freedom, New York: Atheneum, 1967.
[3] Wahyudi Djafar, dkk. 2016. Pelindungan Data Pribadi. Lembaga Studi dan Advokasi Masyarakat (ELSAM). Jakarta.
[4] Bryan A. Garner (ed.), 2004. Black's Law Dictionary, 8th Edition, West Pub. Co, St. Paul.
[5] P. Beynon-Davies, 2002. Information Systems: An Introduction to Informatics in Organisations, Palgrave Macmillan, Basingstoke.
[6] Purwanto, 2007. Penelitian tentang Pelindungan Hukum Data Digital, BPHN Departemen Hukum dan Shinta Dewi Rosadi, 2009. CyberLaw: Pelindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional, Widya Padjadjaran, Bandung.
[7] Nancy Yue Liu, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics, Oxon: Routledge.
[8] Alan F. Westin, Privacy and Freedom, Atheneum, London
[9] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) juncto UU No. 19 Tahun 2016, serta Pasal 84 UU Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.
[10] Budi Rahardjo, Keamanan Informasi di Era Digital, Bandung: Informatika, 2020, hlm. 112.
[11] UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.