



Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Personal Data Protection in the Digital Era Based on Law Number 27 of 2022

Kurdi* & Joko Cahyono

Ilmu Hukum, Fakultas Hukum, Sekolah Tinggi Ilmu Hukum Adhyaksa, Indonesia

Abstrak

Penelitian ini bertujuan untuk membahas konsep data pribadi sebagai hak privasi dalam perspektif hak asasi manusia dan perlindungan hukum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dengan metode penelitian hukum doktrinal, penelitian ini menemukan bahwa UU PDP mengatur perlindungan data pribadi baik secara preventif maupun represif. Perlindungan preventif mencakup pengaturan kewajiban pengendali data untuk menjaga keamanan data pribadi, seperti penerapan sistem keamanan yang memadai dan transparansi pengelolaan data. Sementara itu, perlindungan represif mencakup sanksi administratif dan pidana serta mekanisme yang diterapkan apabila terjadi pelanggaran terhadap perlindungan hukum yang diatur dalam UU PDP. Namun, implementasi perlindungan ini masih menghadapi tantangan besar, terutama terkait dengan penegakan hukum. Belum adanya lembaga khusus yang bertugas menegakkan sanksi dan mengawasi pelaksanaan UU PDP menjadi kendala utama dalam efektivitas perlindungan data pribadi. Oleh karena itu, diperlukan pembentukan lembaga pengawas yang independen untuk memastikan penegakan hukum yang optimal. Penelitian ini menyimpulkan bahwa penguatan regulasi melalui pembentukan lembaga khusus tidak hanya akan memberikan kontribusi signifikan dalam meningkatkan perlindungan hukum terhadap data pribadi di Indonesia, tetapi juga memperkuat kepercayaan masyarakat dalam menghadapi tantangan era digital yang semakin kompleks.

Kata Kunci: Perlindungan Data Pribadi; Hak Asasi Manusia; Hak Privasi.

Abstract

This study examines the concept of personal data as a privacy right from the perspective of human rights and legal protection under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Utilizing doctrinal legal research methods, the study finds that the PDP Law regulates personal data protection both preventively and repressively. Preventive measures include the obligation of data controllers to maintain data security through adequate systems and transparent data management practices. Meanwhile, repressive measures encompass administrative and criminal sanctions, as well as mechanisms to address violations of the legal protections stipulated in the PDP Law. However, the implementation of these protections faces significant challenges, particularly in law enforcement. The absence of a dedicated institution to enforce sanctions and oversee the implementation of the PDP Law represents a major obstacle to ensuring effective personal data protection. Therefore, the establishment of an independent supervisory authority is essential to optimize law enforcement. This study concludes that strengthening regulations through the creation of a specialized institution will not only significantly enhance legal protection for personal data in Indonesia but also bolster public trust in navigating the increasingly complex challenges of the digital era.

Keywords: Personal Data Protection; Human Rights; Privacy Rights.

How to Cite: Kurdi & Cahyono, J. (2024), Perlindungan Data Pribadi di Era Digital Berdasarkan Undang Undang Nomor 27 Tahun 2022. *JUNCTO: Jurnal Ilmiah Hukum*, 6(2): 330-339,

*E-mail: kurdi23001@mail.unpad.ac.id

ISSN 2722-9793 (Online)



PENDAHULUAN

Teknologi terus berkembang pesat sehingga saat ini banyak disebut sebagai era digital. Era digital merujuk pada masa saat mayoritas dari masyarakatnya mempergunakan teknologi digital dalam kehidupan sehari-hari mereka. Era ini telah dimulai sejak 1980an dan terlihat dari terjadinya perubahan besar di mana pada awalnya menggunakan teknologi mekanik dan analog berubah menjadi menggunakan teknologi digital secara masif (Sigulem et al., 2017).

Salah satu teknologi yang mengalami perkembangan secara pesat adalah teknologi informasi. Pesatnya perkembangan teknologi ini mempengaruhi kehidupan masyarakat di berbagai aspek, termasuk di dalamnya terbentuknya ekonomi digital. Ekonomi digital sendiri merupakan kegiatan perekonomian yang berlangsung dengan menggunakan teknologi digital internet. Keberadaan ekonomi digital di Indonesia terlihat dalam masifnya penggunaan *e-commerce*, perbankan digital, transportasi online, dan berbagai jasa yang melibatkan teknologi digital lainnya.

Ekonomi digital membuat transaksi bisnis menjadi lebih mudah, murah, dan cepat. Akan tetapi, terdapat dampak negatif dari ekonomi digital seperti adanya pelanggaran data pribadi dan hak atas privasi (Sihombing, 2022). Hak atas privasi mengacu pada hak seseorang untuk merahasiakan informasi pribadinya, aktivitas pribadinya, atau ruang pribadinya yang tidak menjadi kepentingan atau perhatian publik yang sah (Shao, 2012). Hak atas privasi termasuk dalam hak konstitusional sehingga perlu dilindungi, utamanya di era digital ini.

Penggunaan teknologi informasi dalam berbagai bidang mendorong peningkatan terhadap pengolahan data. Saat ini, banyak aktivitas yang melibatkan penyimpanan data pribadi oleh sistem elektronik. Data pribadi yang tersimpan tersebut meliputi seluruh informasi pribadi yang dapat dipergunakan untuk mengidentifikasi seseorang, misalnya nama, alamat, tanggal lahir, nomor telepon, dan NIK (Suari & Sarjana, 2023). Banyaknya aktivitas yang melibatkan pemrosesan data pribadi di era digital tersebut membuat potensi pelanggaran hak privasi oleh penyelenggara sistem elektronik menjadi semakin tinggi. Potensi pelanggaran hak privasi menjadi semakin tinggi karena sistem keamanan data dari penyelenggara sistem elektronik masih lemah, kurangnya kesadaran dari pemilik data terkait pentingnya menjaga informasi pribadi, dan banyaknya kejahatan *cyber* yang melibatkan pelanggaran data pribadi.

Telah terjadi beberapa kali kejadian kebocoran data pribadi yang termasuk bagian dari privasi seseorang di Indonesia. beberapa kasus tersebut melibatkan kebocoran data publik sehingga jumlah datanya sangat banyak. Kasus-kasus tersebut, seperti kebocoran data BPJS Ketenagakerjaan yang melibatkan 19,56 juta data, kebocoran data Bank Syariah Indonesia yang melibatkan 15 juta data, hingga kebocoran data Dukcapil yang melibatkan 337 juta data penduduk Indonesia (Lintang, 2024). Beberapa kasus tersebut memperlihatkan rentannya pelanggaran data pribadi di Indonesia.

Era digital juga memungkinkan transaksi bisnis menjadi lebih mudah, murah, dan cepat melalui berbagai platform digital seperti *e-commerce*, perbankan digital, dan jasa transportasi online. Namun, perkembangan ini turut menghadirkan dampak negatif, termasuk risiko tinggi terhadap pelanggaran data pribadi yang semakin kompleks seiring meningkatnya kejahatan siber dan lemahnya regulasi pengamanan data.

Melihat pada data yang dihimpun BSSN, pada tahun 2023 kebocoran data di Indonesia masih banyak terjadi di mana di bidang pemerintahan data yang tidak berhasil dilindungi mencapai 665 ribu data, kemudian di bidang keuangan data yang tidak berhasil dilindungi mencapai 165 ribu data, dan di bidang teknologi informasi mencapai 161 ribu data. Data yang tidak berhasil dilindungi tersebut termasuk pula data terkait keputusan pemerintah, data sensitif warga negara, hingga operasi internal pemerintah (Machfir, 2024). Data ini lemahnya perlindungan data di Indonesia, sehingga pemerintah dapat dikatakan belum bisa melindungi data publik sebagaimana seharusnya.

Kebocoran data pribadi dapat menyebabkan kerugian baik secara materiil maupun imateriil. Sebab kebocoran data berpotensi menyebabkan kerugian finansial, mengungkap informasi sensitif, menyebabkan masalah hukum akibat pencurian identitas dan pencemaran nama baik (Kusnadi, 2021). Adanya potensi pelanggaran hak lain yang mengikuti pelanggaran hak privasi membuat peningkatan urgensi perlindungan data pribadi. Selain itu, memang sudah menjadi kewajiban pemerintah untuk memberikan perlindungan dan menjamin keamanan privasi warga negaranya. Kewajiban pemerintah ini secara implisit diatur dalam Pasal 28G ayat 1 UUD 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadinya. Yang berarti bahwa pemerintah mengakui hak privasi sebagai bagian dari hak asasi manusia yang dimiliki oleh setiap orang sehingga harus dilindungi (Manurung, 2023).

Berdasarkan paparan di atas, maka peneliti tertarik membahas lebih lanjut mengenai konsep data pribadi sebagai hak privasi dalam perspektif HAM. Isu ini dibahas berdasarkan perspektif HAM karena hak privasi termasuk dalam salah satu HAM. Selain itu, penelitian ini juga membahas mengenai perlindungan data pribadi sebagai hak privasi dalam era digital pada peraturan perundang-undangan di Indonesia. Isu ini dibahas untuk menganalisis keadaan perlindungan yang diberikan oleh pemerintah dalam hukum yang berlaku. Dari hasil penelitian tersebut, dapat disimpulkan kelebihan dan kekurangan pengaturan hukum terkait perlindungan data pribadi sebagai hak privasi. Dalam hal memang terdapat kekurangan, maka peneliti dapat memberikan masukan untuk reformasi hukum.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada tiga pertanyaan utama. Pertama, bagaimana konsep data pribadi sebagai hak privasi dalam perspektif hak asasi manusia di era digital? Kedua, bagaimana perlindungan hukum terhadap data pribadi sebagai hak privasi di era digital sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi? Ketiga, sejauh mana urgensi pembentukan lembaga pengawas perlindungan data pribadi untuk meningkatkan efektivitas perlindungan hukum terhadap data pribadi di era digital?

METODE PENELITIAN

Penelitian ini menggunakan metode hukum doktrinal dengan pendekatan peraturan perundang-undangan dan konseptual. Menurut Sitabuana (2020) penelitian ini adalah penelitian yang meletakkan hukum sebagai sistem norma, yang berarti hukum dilihat dalam kaitannya dengan norma dari peraturan perundang-undangan, asas, perjanjian, putusan, dan doktrin (Sitabuana, 2020). Pendekatan peraturan perundang-undangan digunakan untuk menganalisis isu hukum berdasarkan peraturan yang relevan, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Hak Asasi Manusia (UU HAM). Pendekatan konseptual diterapkan untuk mendalami konsep-konsep dan teori-teori yang mendasari, seperti konsep data pribadi, hak privasi, dan hak asasi manusia.

Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer dan sekunder. Bahan hukum primer terdiri dari UU PDP, UU HAM, dan peraturan perundang-undangan terkait lainnya. Sementara itu, bahan hukum sekunder mencakup buku, jurnal, skripsi, dan artikel online yang relevan dengan topik penelitian. Teknik pengumpulan data dilakukan melalui studi kepustakaan, yaitu dengan menelaah literatur dan dokumen yang relevan untuk menjawab permasalahan penelitian.

Analisis dalam penelitian ini dilakukan secara kualitatif, yaitu dengan menafsirkan bahan hukum yang telah dikumpulkan dan diolah sebelumnya. Analisis ini bertujuan untuk menghasilkan kesimpulan yang dapat memberikan kontribusi terhadap pengembangan hukum perlindungan data pribadi di era digital. Penyesuaian ini memastikan struktur lebih sederhana dan menghindari repetisi, sesuai dengan saran revisi (Syafitri et al., 2024).

HASIL DAN PEMBAHASAN

Konsep Data Pribadi Sebagai Hak Privasi dalam Perspektif Hak Asasi Manusia di Era Digital

Hak asasi manusia adalah hak yang melekat dalam sifat manusia dan tanpa hak itu manusia tidak dapat hidup sebagai makhluk beradab. Budiardjo menyatakan bahwa HAM merupakan hak yang dimiliki setiap manusia dan melekat pada manusia karena ia manusia. Penjelasan mengenai HAM dalam pasal 1 angka 1 UU No. 39 Tahun 1999 Tentang HAM adalah:

“Seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai makhluk Tuhan YME dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara, hukum, Pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia;”

Salah satu HAM adalah hak privasi dan ini telah diakui secara internasional. pengakuan secara internasional terhadap hak privasi dapat ditemukan dalam Deklarasi Universal Hak Asasi Manusia, utamanya pada Pasal 12 yang menyatakan: “Tidak seorang pun boleh diganggu secara sewenang-wenang dalam urusan pribadi, keluarga, rumah, atau surat-menyuratnya, atau diserang atas kehormatan dan nama baiknya. Setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam ini (McCarthy, 2012). Sementara di Indonesia sendiri dasar perlindungan hak privasi terkandung secara implisit dalam Pasal 28G ayat 1 UUD 1945. Dalam pasal tersebut dijamin bahwa setiap orang memiliki hak atas perlindungan diri pribadinya, kehormatan, martabat, dan hak untuk merasa aman dari ancaman ketakutan untuk memilih berbuat suatu hal atau tidak berbuat suatu hal yang asasi (Fauzy & Shandy, 2022). Jaminan perlindungan tersebut adalah esensi dari hak atas privasi yang melindungi berbagai aspek agar seseorang memperoleh perlindungan dan terbebas dari ancaman ketakutan.

Privasi sendiri adalah kerahasiaan pribadi yang tidak memiliki hubungan dengan masalah kepentingan publik. Privasi terdiri dari 3 aspek, yaitu informasi pribadi, aktivitas pribadi, dan juga ruang pribadi. Aspek pertama, yakni informasi pribadi merujuk pada seluruh data dan informasi milik individu, seperti nama, alamat, tinggi badan, nomor telepon, wajah, pengalaman hidup, hingga catatan medisnya. Aspek kedua yakni aktivitas pribadi merujuk pada keseluruhan kegiatan individu yang tidak ingin dipublikasikan, seperti kehidupan seksualnya, jadwal harian, interaksi sosial, dsb. Sementara ruang pribadi merujuk pada rahasia yang dimiliki oleh individu seperti bagian tubuh yang ia rahasiakan, ruang virtualnya, buku hariannya (McCarthy, 2012).

Hak privasi merupakan hak penting yang melindungi martabat manusia dan mendasari hak asasi lainnya. Privasi melindungi individu dari gangguan dan ancaman, serta memengaruhi hubungan sosial mereka (Lesmana et al., 2021). Menurut Kusnadi, hak privasi mendukung hubungan sosial dengan menjaga aspek tertentu dari kehidupan pribadi individu (Kusnadi, 2021). Pelanggaran privasi dapat menyebabkan kerugian imateriil yang berdampak signifikan pada kehidupan korban, termasuk hubungan mereka dengan masyarakat. Hak privasi mencakup empat aspek utama: hidup tenang dan damai tanpa penguntitan atau perekaman ilegal; pengendalian atas informasi pribadi seperti kesehatan dan status perkawinan; kerahasiaan komunikasi seperti percakapan telepon dan e-mail; serta pemanfaatan privasi untuk kepentingan komersial atau non-komersial sesuai hukum.

Salah satu aspek dari hak atas privasi adalah mengenai informasi pribadinya atau data pribadi setiap orang. Perlindungan hak privasi terkait hal ini menjadi semakin berkembang sehingga dirumuskan perlindungan data pribadi (Priscyllia, 2019). Perlindungan data pribadi ini menjadi semakin penting di era digital saat ini. Sebab banyak kegiatan dilakukan secara digital yang melibatkan data pribadi. Data pribadi seperti nama lengkap, NIK, nomor rekening, PIN ATM,

digunakan dalam kegiatan digital tersebut. Dalam hal tidak dilindungi, maka data pribadi tersebut dapat disalahgunakan untuk tindakan yang dapat merugikan pemilik data pribadi. Beberapa contoh kejahatan yang melibatkan data pribadi dan melanggar hak privasi di era digital misalnya *doxing* di media sosial saat menggunakan hak kebebasan berpendapat, *revenge porn*, penyalahgunaan identitas untuk melakukan berbagai bentuk kejahatan *cyber*, penggunaan data pribadi untuk melakukan *carding*, *phising* untuk mencuri uang di rekening bank, dsb. Hal ini memperlihatkan bahwa perlindungan data pribadi juga penting untuk mencegah pelanggaran HAM yang jauh lebih besar.

Dilihat dari klasifikasinya, hak privasi itu bagian dari *derogable rights*. Sebab tidak termasuk dalam bagian dari *nonderogable rights* sebagaimana dimaksud pada 28 ayat 1 UUD 1945. Yang berarti bahwa pemenuhan hak privasi dapat dikurangi atau dibatasi. Akan tetapi pengurangannya harus mengikuti hukum yang berlaku, seperti aturan terkait penyadapan, penyiaran, dsb. Dengan demikian, pengurangan pemenuhan hak privasi hanya dapat dilakukan pada situasi khusus atau ditentukan secara limitatif dengan undang-undang.

Perlindungan Hukum Terhadap Data Pribadi sebagai Hak Privasi dalam Era Digital pada Peraturan Perundang-Undangan di Indonesia

Perlindungan hukum merupakan keseluruhan langkah hukum yang seharusnya dilakukan oleh instansi penegak hukum untuk memberikan keamanan secara psikologis dan secara fisik dari ancaman berbagai pihak. perlindungan hukum sendiri terbagi menjadi 2 perspektif, yakni perlindungan secara preventif dan juga secara represif. Adapun perlindungan preventif merujuk pada berbagai aturan dalam peraturan perundang-undangan yang isinya berupa kewajiban atau membatasi tingkah laku agar tidak terjadi pelanggaran hak orang lain. sementara perlindungan preventif adalah perlindungan yang diberikan dalam bentuk penyelesaian sengketa akibat terjadinya pelanggaran.

Perlindungan data pribadi di Indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Untuk selanjutnya disebut sebagai UU PDP). Berdasarkan pasal 1 angka 2 UU PDP dapat diketahui bahwa perlindungan data pribadi merupakan seluruh upaya yang dilakukan untuk memberikan perlindungan terhadap data pribadi yang ada pada rangkaian pemrosesan data pribadi untuk menjamin hak konstitusional dari pemilik data pribadi tersebut.

Dalam UU PDP diatur berbagai hak pemilik data pribadi dan kewajiban, serta tanggung jawab dari pengendali data pribadi dan juga prosesor data pribadi atas data pribadi yang dikelolanya. Aturan-aturan tersebut termasuk dalam perlindungan hukum preventif karena mencegah terjadinya pelanggaran data pribadi sebagai bagian dari hak privasi seseorang. Beberapa hak dari pemilik data pribadi diatur dalam Bab IV yang mengatur terkait hak subjek data pribadi. Dalam pasal 5 diatur bahwa pemilik data pribadi memiliki hak atas informasi terkait identitas dan juga dasar kepentingan pengumpulan dan penggunaan data pribadi yang diminta. Selain itu, pemilik data pribadi memiliki hak untuk memilih mengakhiri dan menarik kembali pemrosesan data dan menghapus data tersebut sesuai dengan peraturan perundang-undangan.

Dalam pasal 10, diatur pula bahwa pemegang data pribadi berhak untuk menyatakan keberatan atas pengambilan keputusan yang hanya berdasarkan pada pemrosesan secara otomatis hingga berakibat hukum terhadap pemilik data pribadi tersebut. dalam hal hak ini dilanggar, dalam pasal 12 diatur bahwa pemilik data pribadi dapat mengajukan gugatan dan memperoleh ganti kerugian dari terjadinya pelanggaran pemrosesan data pribadi dirinya tersebut. Dalam pasal 13 diatur bahwa pemilik data pribadi berhak menggunakan data pribadinya dari pengendali data pribadi dalam format yang umum digunakan atau dibaca oleh sistem elektronik. Berbagai hak tersebut menunjukkan bahwa terdapat perlindungan hukum melalui penjaminan hak yang berkaitan dengan pemrosesan data pribadi oleh pengendali data pribadi.

Pengecualian dari hak-hak yang dimiliki oleh pemilik data pribadi terjadi apabila berkaitan dengan kepentingan pertahanan dan keamanan nasional, dilakukannya penegakan hukum, untuk kepentingan penyelenggaraan negara, pengawasan sektor moneter, jasa keuangan, sistem

pembayaran, dan stabilitas sistem keuangan yang dijalankan untuk kepentingan negara, dan apabila digunakan untuk statistik dan penelitian ilmiah.

Selain mengatur mengenai hak pemilik data pribadi, diatur pula kewajiban pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi. Kewajiban-kewajiban tersebut diatur agar hak pemilik data pribadi dipenuhi oleh pengendali data pribadi dalam kegiatan pemrosesan data pribadi. Pengendali Data Pribadi dan Prosesor Data Pribadi sendiri berdasarkan pasal 19 dapat berupa perseorangan, badan publik, dan juga organisasi internasional. dalam melakukan kegiatan pemrosesan data pribadi tersebut, pengendali data pribadi haruslah memiliki dasar, yang berupa: pertama, persetujuan pemilik data pribadi untuk pemrosesan data demi tujuan yang dinyatakan secara jelas. Kedua, memenuhi kewajiban hukum dari pengendali data sesuai dengan hukum yang berlaku. ketiga, melindungi kepentingan vital pemilik data pribadi. Keempat, melaksanakan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan hukum yang berlaku, dan memenuhi kepentingan sah lain dengan mempertimbangkan keseimbangan kepentingan Pengendali Data Pribadi dan hak pemilik data pribadi.

Apabila pemrosesan data pribadi itu dilakukan dari adanya persetujuan, maka pengendali data diwajibkan untuk memberikan informasi terkait legalitas pemrosesan data, tujuan pemrosesan, jenis dan relevansi data, waktu retensi dokumen, perincian berbagai informasi yang disimpan, jangka waktu pemrosesan, dan juga hak dari pemilik data pribadi. Apabila terdapat perubahan informasi, pengendali data pribadi juga diwajibkan untuk melaporkan perubahan tersebut sebelum dilakukannya perubahan data kepada pemilik data pribadi yang bersangkutan. persetujuan pemrosesan data ini dapat dilakukan melalui perjanjian tertulis atau terekam. Jika dalam perjanjian tersebut terdapat tujuan lain atau permintaan lain, maka haruslah dituliskan dalam format yang mudah dipahami dan mudah diakses dengan bahasa yang sederhana dan jelas. Dalam hal pada perjanjian tersebut tidak termuat persetujuan yang sah dan disebutkan secara eksplisit, maka akan dianggap batal demi hukum (pasal 23).

Dalam hal pemrosesan data pribadi itu dilakukan terhadap pemilik data pribadi yang termasuk golongan anak ataupun penyandang disabilitas, maka penyelenggaraannya dilakukan secara khusus. Yang mana wajib memperoleh persetujuan dari orang tua atau walinya sesuai dengan peraturan perundang-undangan yang berlaku.

Pengendali data pribadi wajib menolak apabila orang lain selain pemilik data pribadi meminta akses terhadap data pribadi apabila permintaan akses tersebut dapat berakibat membahayakan keamanan, kesehatan fisik, ataupun psikis dari pemilik data pribadi, berakibat terungkapnya data pribadi milik orang lain, dan apabila tidak sesuai dengan kepentingan pertahanan dan keamanan negara.

Dengan maksud memberikan perlindungan terhadap keamanan data pribadi, maka pengendali data juga diwajibkan untuk memastikan keamanan data pribadi yang mereka proses. Kewajiban ini dilakukan dengan menyusun dan menerapkan langkah teknis operasional untuk memberikan perlindungan terhadap data pribadi dari segala bentuk ancaman dan gangguan pemrosesan data pribadi yang bertentangan dengan hukum yang berlaku, seperti ancaman *hacking* dan *cyber crime* lainnya. Selain itu, pengendali data pribadi juga diwajibkan untuk menentukan tingkat keamanan berdasarkan sifat dan risiko data yang mereka simpan.

Demi terjaminnya kerahasiaan data pribadi, pengendali data wajib merahasiakan data pribadi dan melakukan pengawasan terhadap seluruh pihak yang terlibat dalam pemrosesan data pribadi di bawah kendalinya. Selain itu, juga harus melindungi data pribadi tersebut dari terjadinya pemrosesan data yang tidak sah dan juga mencegah data tersebut diakses secara tidak sah. Untuk itu, pengendali data pribadi wajib memproses Data Pribadi sistem elektronik secara andal, aman, dan bertanggung jawab. Tata cara perlindungan data pribadi oleh pengendali data pribadi tersebut diatur lebih lanjut dalam Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Untuk memberikan perlindungan terhadap data pribadi, maka Pengendali Data Pribadi haruslah mengakhiri pemrosesan data pribadi jika masa retensi telah selesai, tujuan pemrosesan data pribadi telah terpenuhi, dan apabila ada permintaan dari pemilik data pribadi. Selanjutnya, pengendali data pribadi akan diwajibkan melakukan penghapusan data.

Pengendali data pribadi yang gagal memberikan perlindungan data pribadi harus melaporkan kejadian tersebut secara tertulis paling telat 3 x 24 jam kepada pemilik data pribadi. Dalam laporan tersebut disebutkan data pribadi yang bocor, kronologis kebocoran data, dan upaya penanganan serta pemulihan akibat kebocoran data tersebut.

Kewajiban dan juga tanggung jawab pengendali data pribadi sebagaimana dijelaskan sebelumnya itu juga dibebankan kepada prosesor data pribadi. Pembebanan kewajiban ini untuk mencegah terjadinya kebocoran data yang melanggar hak privasi seseorang. Batasan berupa larangan-larangan untuk memberikan perlindungan hukum dari terjadinya penyalahgunaan data pribadi diatur dalam Bab XIII UU PDP. Dalam aturan tersebut, diatur berbagai bentuk tindak pidana terkait penyalahgunaan data pribadi.

Selain memberikan perlindungan secara preventif, UU PDP juga memberikan perlindungan secara represif. Yang berarti diatur perlindungan hukum berupa penyelesaian sengketa dari adanya pelanggaran data pribadi sebagai bagian dari hak privasi. Hal ini terlihat dalam aturan mengenai sanksi dan juga mekanisme penyelesaian sengketa pelanggaran data pribadi. Di mana dalam hal pengendali data pribadi dan prosesor data pribadi melakukan pelanggaran dengan tidak menjalankan tanggung jawab dan kewajibannya, maka dapat dikenai sanksi administratif. Sanksi administratif yang dapat dikenakan terhadap pelanggar mulai dari peringatan tertulis, kemudian dihentikannya dalam jangka waktu tertentu kegiatan pemrosesan Data Pribadi, penghapusan data pribadi, dan juga penjatuhan denda administratif. Denda yang dapat diberikan ini maksimal 2% dari pendapatan tahunan atau dari jumlah penerimaan tahunan terhadap faktor pelanggaran. Penjatuhan sanksi administratif tersebut akan dilakukan oleh lembaga yang bertugas memberikan perlindungan data pribadi. Akan tetapi, lembaga ini masih belum terbentuk di Indonesia. meskipun pasal 58 ayat 1 UU PDP mengamanatkan agar presiden perlu segera menetapkan pembentukan lembaga ini melalui peraturan presiden.

Dalam pasal 64 UU PDP, diatur bahwa penyelesaian sengketa perlindungan data pribadi dapat diselesaikan melalui arbitrase, pengadilan, atau dapat pula melalui lembaga alternatif penyelesaian sengketa lainnya. adapun tata cara penyelesaian sengketa tersebut dilaksanakan sesuai dengan hukum acara dari lembaga yang menyelesaikan sengketa.

Adapun untuk menegakkan larangan-larangan terkait penyalahgunaan data pribadi, diatur sanksi-sanksi untuk menyelesaikan pelanggaran, yang antara lain:

- a. Larangan untuk setiap orang secara melawan hukum mengumpulkan data pribadi yang bukan miliknya untuk keuntungan pribadinya atau orang lain sehingga berakibat kerugian bagi pemilik data pribadi (pasal 65 ayat 1). Dalam hal dilanggar, dikenakan sanksi sebagaimana diatur dalam pasal 67 ayat 1 UU PDP yakni pidana penjara maksimal 5 tahun dan/atau denda maksimal 5 miliar rupiah.
- b. Larangan mengungkapkan data pribadi milik orang lain secara melawan hukum (Pasal 65 ayat 2). Dalam hal dilanggar, maka diancam pidana maksimal 4 tahun dan/atau pidana denda maksimal 4 miliar rupiah.
- c. larangan menggunakan data pribadi orang lain secara melawan hukum (pasal 65 ayat 3). Yang apabila dilanggar diancam pidana penjara maksimal 5 tahun dengan denda maksimal 5 miliar rupiah.
- d. Larangan dengan sengaja membuat data pribadi palsu untuk keuntungan pribadinya atau orang lain sehingga berakibat kerugian terhadap orang lain (pasal 66). Yang apabila dilanggar diancam pidana maksimal 6 tahun dan/atau pidana denda maksimal 6 miliar rupiah.

Berdasarkan paparan di atas, dapat diketahui bahwa perlindungan hukum secara represif tidak hanya mengatur sanksi pelanggaran dari sanksi administratif saja, melainkan juga dapat melalui pengadilan perdata dan bahkan melalui penegakan hukum pidana. mekanisme penyelesaian sengketa yang disediakan juga tidak hanya di pengadilan, melainkan juga dapat diselesaikan di luar pengadilan tergantung pada sengketa yang terjadi.

Perlunya Pembentukan Lembaga Perlindungan Data Pribadi untuk Meningkatkan Perlindungan Terhadap Data Pribadi sebagai Hak Privasi di Era Digital

Dalam Pasal 58 UU PDP dijelaskan bahwa pemberian perlindungan data pribadi dilakukan oleh lembaga yang akan ditetapkan oleh Presiden melalui peraturan Presiden. Yang berarti bahwa UU mengamatkan pembentukan lembaga pengawas terkait perlindungan data pribadi. Berdasarkan pasal 59 UU PDP disebutkan bahwa lembaga tersebut bertanggung jawab melakukan perumusan kebijakan dan strategi untuk memberikan perlindungan data pribadi yang kemudian akan digunakan sebagai pedoman oleh pemilik data pribadi, pengendali data pribadi, dan juga prosesor data pribadi. Lembaga ini juga bertugas melakukan pengawasan terhadap penyelenggaraan perlindungan data pribadi, menegakkan hukum administratif atas pelanggaran terhadap UU PDP, dan mendorong penyelesaian sengketa di luar pengadilan.

Lembaga perlindungan data pribadi ini diperlukan untuk menjalankan kewenangan dalam membantu penegak hukum dalam menangani dugaan tindak pidana yang diatur dalam UU PDP, menjalin kerja sama dengan lembaga PDP lain untuk menyelesaikan pelanggaran UU PDP yang dilakukan secara lintas negara, menindaklanjuti hasil pengawasan terhadap sistem keamanan pengendali data pribadi, menerima laporan terkait dugaan pelanggaran data pribadi, memeriksa laporan tersebut, dan menyelesaikan dugaan pelanggaran dengan memanggil para pihak yang terkait dengan pelanggaran, serta melakukan konsultasi hukum dengan kejaksaan terkait penyelesaian sengketa PDP.

Ketiadaan lembaga ini membuat perlindungan hukum yang terdapat dalam UU PDP belum bisa dilaksanakan dengan baik. Sebab belum ada lembaga yang menjalankan pelanggaran hukum terhadap UU PDP, utamanya penegakan sanksi administratif yang menjadi kewenangan dari Lembaga Perlindungan Data Pribadi.

Lembaga Perlindungan Data Pribadi belum juga dibentuk meskipun UU PDP telah diundangkan sejak 17 Oktober 2022 lalu. Padahal, dari pengundangan UU PDP hingga saat ini telah terjadi banyak kebocoran data pribadi yang melanggar hak privasi warga negara Indonesia. Banyak kebocoran data pribadi tersebut membuat kepercayaan masyarakat terhadap perlindungan data oleh pemerintah semakin menurun. Salah satunya kejadian yang menyebabkan penurunan kepercayaan masyarakat terhadap pemerintah adalah terjadinya serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS). Serangan ini menyebabkan terkuncinya data dari 282 kementerian/lembaga pemerintah. Kasus ini bahkan disebut sebagai kebocoran data terparah dalam sejarah serangan terhadap data pemerintah (Machfir, 2024).

Membandingkan dengan beberapa negara lain yang juga memiliki undang-undang khusus terkait perlindungan data pribadi. Mereka telah memiliki lembaga khusus untuk melakukan pengawasan terhadap perlindungan data pribadi. Berikut penjabaran yang menunjukkan perbandingan dengan beberapa negara yang telah memiliki lembaga khusus perlindungan data pribadi:

- a. Perancis mengatur perlindungan data pribadi melalui *Loi Informatique et Libertés* atau *The French Data Protection Act* (FDPA) yang disahkan sejak 6 Januari 1978. FDPA mengalami beberapa kali amandemen untuk menyesuaikan dengan era digital dan terakhir diamandemen untuk mengharmonisasikannya dengan General Data Protection Regulation (GDPR) yang dibentuk oleh Uni Eropa. Perancis telah memiliki lembaga khusus yang menangani perlindungan data pribadi yakni *Commission nationale de l'informatique et des libertés* (CNIL). Lembaga tersebut merupakan otoritas administratif independen yang melakukan pengawasan terhadap perlindungan data pribadi secara nasional di Perancis.
- b. Korea Selatan mengatur perlindungan data pribadinya melalui *Personal Information Protection Act* (PIPA) 2011. Untuk menegakkan aturan dalam UU tersebut, di Korea Selatan dibentuk *Personal Information Protection Commission* (PIPC). Komisi ini merupakan badan administratif pusat di bawah Presiden yang melaksanakan tugasnya secara independen.
- c. Singapura mengatur perlindungan data pribadinya melalui *Personal Data Protection Act* (PDPA) 2012. Untuk melakukan pengawasan dan menjamin perlindungan data pribadi telah dibentuk *Personal Data Protection Commission Singapore* (PDPC). PDPC berada pada lembaga yang telah ada sebelumnya, yakni *The Info-communications and Media Development Authority* (IMDA) (Khansa, 2021).

Melihat pada perbandingan dengan beberapa negara tersebut, dapat diketahui bahwa setelah pengesahan UU PDP, pemerintah Indonesia perlu segera melakukan pembentukan Lembaga Perlindungan Data Pribadi. Dari perbandingan tersebut, dapat diketahui bahwa pemerintah dapat memilih membentuk lembaga perlindungan data pribadi sebagai lembaga independen yang berdiri sendiri secara khusus atau dengan menggabungkan kewenangan tersebut pada lembaga yang telah ada. Melihat bahwa pada pasal 58 UU PDP bahwa pemerintah memiliki peranan mewujudkan perlindungan pribadi sesuai UU PDP dan dilaksanakan oleh lembaga yang ditetapkan oleh Presiden dan bertanggung jawab kepada Presiden, maka lembaga Perlindungan Data Pribadi yang akan dibentuk oleh pemerintah nantinya akan berada di bawah Presiden.

Mengingat bahwa perlindungan data pribadi ini mencakup pengendalian data sektor publik, maka menurut peneliti seharusnya lembaga perlindungan data pribadi dibentuk sebagai lembaga independen non kementerian yang secara khusus menjalankan aturan dalam UU PDP. Artinya, lembaga ini secara struktural tidak ditempatkan di bawah presiden ataupun kementerian untuk mempertahankan independensinya. Akan tetapi, dikarenakan proses politik telah menempatkan lembaga perlindungan data pribadi sebagai lembaga yang bertanggung jawab kepada Presiden, maka sebaiknya lembaga PDP dijadikan sebagai bagian dari pemerintahan lainnya yang tidak memiliki hubungan fungsional terhadap menteri yang mengkoordinasikannya (Kominfo) (*Lembaga Perlindungan Data Pribadi, Kunci Penegakan Kepatuhan UU PDP*, 2024). Selain itu, aturan mengenai pengangkatan dan pemberhentian dari pimpinan lembaga perlu diatur dengan ketat melalui syarat tertentu, sehingga tidak dapat diangkat dan diberhentikan berdasarkan alasan politis saja. Dengan keberadaan lembaga perlindungan data pribadi yang independen dan menjalankan tugasnya sesuai dengan UU PDP ini, diharapkan tidak terjadi pelanggaran hak privasi dari warga negara Indonesia.

SIMPULAN

Kesimpulan penelitian ini menegaskan bahwa data pribadi merupakan bagian integral dari hak privasi, yang juga diakui sebagai hak asasi manusia dalam Pasal 12 DUHAM. Perlindungan terhadap hak privasi semakin mendesak di era digital mengingat banyaknya aktivitas yang melibatkan data pribadi serta risiko penyebaran data melalui media sosial. Di Indonesia, perlindungan hukum terhadap data pribadi diatur secara khusus dalam UU PDP, yang mencakup perlindungan preventif dan represif. Perlindungan preventif meliputi hak-hak pemilik data pribadi, kewajiban dan tanggung jawab pengendali serta prosesor data pribadi, serta larangan terhadap pelanggaran privasi seperti penyebaran dan penyalahgunaan data pribadi. Perlindungan represif, di sisi lain, menyediakan sanksi dan mekanisme penegakan hukum untuk menindak pelanggaran yang terjadi.

Perlindungan represif ini belum optimal karena belum adanya lembaga khusus yang bertugas melaksanakan UU PDP. Lembaga ini diperlukan untuk membentuk pedoman perlindungan, mengawasi pengendalian dan pemrosesan data pribadi, serta menindak pelanggaran. Kondisi ini menyebabkan kasus-kasus kebocoran data pribadi di Indonesia belum tertangani secara memadai dan terus berulang.

Untuk meningkatkan efektivitas perlindungan data pribadi, pemerintah perlu segera membentuk lembaga perlindungan data pribadi yang independen. Lembaga ini harus memiliki kewenangan penuh untuk menegakkan UU PDP, mengawasi implementasi pedoman perlindungan, serta memberikan edukasi kepada masyarakat tentang pentingnya menjaga privasi di era digital.

REFERENSI

- Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445–461.
- Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, 2(8), 649–662.
- Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, 2(1), 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>

- Lembaga Perlindungan Data Pribadi, Kunci Penegakan Kepatuhan UU PDP.* (2024). Lembaga Studi & Advokasi Masyarakat.
- Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 3(2), 1–6.
- Lintang, I. (2024). *10 Kasus Kebocoran Data di Indonesia yang Paling Menggemparkan*. Inilah.Com.
- Machfir, Z. (2024). *300 Juta Data Pribadi Tersebar, Kapan Indonesia Merdeka dari Serangan Siber?* GoodStats.
- Manurung, E. A. P. (2023). The Right to Privacy Based on The Law of The Republic of Indonesia Number 27 of 2022. *Journal of Digital Law and Policy*, 2(3), 103–110.
- McCarthy, P. (2012). Privacy, Challenges to. In *Encyclopedia of Applied Ethics* (pp. 599–608). Elsevier. <https://doi.org/10.1016/B978-0-12-373932-2.00300-8>
- Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, 34(3), 239–249.
- Shao, G. (2012). Privacy interests. In *Internet Law in China* (pp. 141–182). Elsevier. <https://doi.org/10.1016/B978-1-84334-648-7.50004-2>
- Sigulem, D., Ramos, M. P., & de Holanda Albuquerque, R. (2017). The New Medicine. In *Global Health Informatics* (pp. 152–167). Elsevier. <https://doi.org/10.1016/B978-0-12-804591-6.00008-2>
- Sihombing, Y. F. T. (2022). *Tinjauan Perbandingan Regulasi Perlakuan Pajak Pertambahan Nilai atas Transaksi Digital di Indonesia, Inggris, dan Prancis*. Politeknik Keuangan Negara.
- Sitabuana, T. H. (2020). *Hukum Tata Negara Indonesia*. Konstitusi Press.
- Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142.
- Syafitri, C. Z., Kurdi, K., Rusli, B., & Azhari, A. (2024). Land Rights and Their Environmental Implications for Indigenous Communities in Nusantara Capital City. *Jurnal Hukum Magnum Opus*, 7(2), 198–209. <https://doi.org/10.30996/jhmo.v7i2.11569>