e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 12 No 11 Tahun 2025 Hal. : 4416-4430

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

DARI RECTSVACCUM MENUJU KEPASTIAN HUKUM: PEMBENTUKAN LEMBAGA PERLINDUNGAN DATA PRIBADI SEBAGAI PENEMUAN HUKUM DI ERA DIGITAL

Muhammad Putra Syawal Al Mahdi, Irwan Triadi

Magister Hukum Fakultas Hukum, Universitas Pembangunan Negeri Veteran

Abstrak

Ketiadaan lembaga otoritatif dalam sistem perlindungan data pribadi di Indonesia menimbulkan kekosongan otoritas (rechtsvacuum) yang berdampak pada lemahnya implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Penelitian ini bertujuan untuk menganalisis urgensi pembentukan Lembaga Pelindungan Data Pribadi (Lembaga PDP) sebagai bentuk penemuan hukum (rechtsvinding) di era digital, sekaligus merumuskan desain kelembagaan ideal yang sesuai dengan prinsip negara hukum yang demokratis. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif terhadap sistem perlindungan data pribadi di Malaysia, Singapura, Hongkong, dan Jepang. Hasil penelitian menunjukkan bahwa tanpa adanya lembaga independen, pelaksanaan UU PDP hanya bersifat normatif tanpa daya paksa dan mekanisme pengawasan yang efektif. Model kelembagaan seperti Independent Regulatory Agencies dinilai paling relevan untuk diterapkan di Indonesia karena menjamin independensi struktural, fungsional, dan institusional dari pengaruh kekuasaan eksekutif. Oleh karena itu, pembentukan Lembaga PDP merupakan kebutuhan mendesak untuk memastikan keadilan, kepastian hukum, dan perlindungan hak asasi warga negara dalam ekosistem digital.

Kata Kunci: Perlindungan Data Pribadi, Lembaga PDP, Penemuan Hukum, Independensi, Era Digital.

PENDAHULUAN

Perkembangan teknologi digital dewasa ini telah mengubah secara fundamental lanskap kehidupan masyarakat Indonesia di berbagai bidang, mulai dari ranah sosial, ekonomi, hingga tata kelola pemerintahan (Pohan & Nasution, 2023). Dinamika digitalisasi

*Correspondence Address : putraalmahdi99@gmail.com
DOI : 10.31604/jips.v12i11.2025. 4416-4430

tersebut melahirkan era baru yang ditandai dengan mobilitas data lintas batas negara yang semakin masif, di mana arus informasi tidak lagi terikat pada batas geografis atau yurisdiksi tertentu (Lie et al., 2022). Dalam konteks ini, data pribadi memperoleh kedudukan yang sangat strategis—tidak semata sebagai representasi identitas seseorang, melainkan telah menjelma menjadi komoditas bernilai tinggi yang memiliki dimensi ekonomi sekaligus politik. Nilai data pribadi kini terletak pada potensinya untuk digunakan sebagai instrumen dalam proses analisis dan pengambilan keputusan, baik dalam penyusunan kebijakan publik maupun dalam strategi bisnis sektor swasta (Dewi, 2016). Mengacu pada hal tersebut, data pribadi telah bergeser dari sekadar informasi individual menuju aset strategis yang menjadi fondasi utama bagi pengembangan kebijakan berbasis bukti, inovasi ekonomi digital, serta peningkatan efisiensi tata kelola pemerintahan modern.

Sebagai sesuatu yang memiliki nilai strategis dan bernilai tinggi di era digital, data pribadi menempati posisi yang sangat vital dalam kehidupan masyarakat modern. Oleh karena itu, upaya untuk melindungi data pribadi menjadi suatu keniscayaan hukum yang tidak dapat diabaikan, mengingat potensi penyalahgunaannya dapat menimbulkan konsekuensi serius terhadap hak privasi, keamanan, serta martabat individu. Menyadari urgensi tersebut, negara melalui pemerintah telah mengambil langkah progresif dengan menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (selanjutnya disebut "UU PDP") (Matheus & Gunadi, 2024). Kehadiran regulasi ini menandai tonggak penting dalam sistem hukum nasional, karena untuk pertama kalinya Indonesia memiliki payung hukum yang komprehensif, sistematis, dan setara dengan rezim perlindungan data di tingkat global. UU PDP tidak hanya mengatur tentang hak dan kewajiban para pihak yang terlibat dalam pemrosesan data pribadi, tetapi juga menegaskan peran negara dalam menjamin keseimbangan antara kebutuhan inovasi teknologi dan perlindungan hak fundamental warga negara atas privasinya di ruang digital.

Meskipun Pemerintah telah mengesahkan UU PDP sebagai tonggak penting dalam penguatan hak privasi individu, implementasinya belum sepenuhnya optimal. Hal ini disebabkan karena belum terbentuknya lembaga otoritatif sebagaimana diamanatkan dalam Pasal 58 ayat (2) UU PDP, yang berfungsi untuk melakukan pengawasan, penegakan hukum, serta penyelesaian sengketa di bidang pelindungan data pribadi. Ketiadaan lembaga tersebut menimbulkan kesenjangan antara norma hukum yang telah ditetapkan dengan mekanisme pelaksanaannya di lapangan. Kondisi ini menunjukkan bahwa perlindungan data pribadi di Indonesia masih berada pada tahap transisi normatif menuju sistem kelembagaan yang kuat dan independen. Dalam konteks ini, urgensi pembentukan lembaga pelindungan data pribadi menjadi semakin penting, tidak hanya untuk memastikan efektivitas pelaksanaan UU PDP, tetapi juga untuk menegaskan komitmen negara dalam menjamin hak konstitusional warga negara atas privasi di era digital yang semakin kompleks.

Ketiadaan lembaga khusus yang berwenang dalam perlindungan data pribadi mengakibatkan terjadinya kekosongan otoritas (*rechtsvacuum*) yang berdampak langsung pada ketidakpastian hukum serta melemahnya perlindungan hak warga negara atas privasi digital. Kekosongan ini menciptakan kondisi di mana mekanisme penegakan hukum dan

pengawasan terhadap pelanggaran data pribadi menjadi tidak efektif, sehingga membuka ruang bagi berbagai bentuk pelanggaran seperti kebocoran data, penyalahgunaan informasi pribadi oleh pihak yang tidak berwenang, serta transfer data lintas batas tanpa pengawasan dan akuntabilitas yang memadai. Dalam perspektif negara hukum yang demokratis, keadaan tersebut jelas bertentangan dengan prinsip kepastian hukum (*legal certainty*) dan proses hukum yang adil (*due process of law*), karena negara seharusnya menjamin adanya struktur kelembagaan yang mampu menegakkan hak privasi digital warga negara secara efektif dan akuntabel di tengah pesatnya perkembangan teknologi informasi.

Di sisi lain, pembentukan Lembaga PDP memiliki nilai strategis sebagai bentuk *rechtsvinding* atau penemuan hukum di era digital. Penemuan hukum diperlukan ketika norma yang ada belum cukup untuk menjawab tantangan baru yang muncul dari perkembangan teknologi. Sebagai lembaga independen, Lembaga PDP diharapkan menjadi penjamin transparansi, akuntabilitas, dan efektivitas penegakan hukum di bidang PDP. Melalui kajian komparatif terhadap model kelembagaan di Malaysia, Singapura, Hongkong, dan Jepang, penelitian ini berupaya merumuskan desain kelembagaan ideal yang mampu menjamin perlindungan hak privasi sekaligus memperkuat posisi Indonesia dalam tata kelola data global.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu suatu metode penelitian hukum yang berfokus pada kajian terhadap norma-norma hukum positif yang berlaku serta prinsip-prinsip hukum yang relevan dengan permasalahan yang diteliti (Marzuki, 2019). Penelitian yuridis normatif berfokus pada penelaahan terhadap bahan-bahan hukum yang berfungsi sebagai dasar dalam menganalisis dan menafsirkan fenomena hukum yang terjadi, dalam hal ini mengenai pembentukan Lembaga PDP sebagai penemuan hukum di era digital.

Data yang digunakan dalam penelitian ini merupakan data sekunder, yang diperoleh melalui studi kepustakaan (*library research*). Data sekunder tersebut terdiri atas bahan hukum primer, yaitu peraturan perundang-undangan yang relevan seperti UU PDP dan serta peraturan lainnya yang terkait dengan tata kelola data pribadi di Indonesia. Selain itu, penelitian ini juga menggunakan bahan hukum sekunder berupa literatur, buku, jurnal ilmiah, hasil penelitian, artikel hukum, serta dokumen akademik yang memberikan penjelasan dan analisis mengenai konsep perlindungan data pribadi, kelembagaan, dan *rechtsvinding* (penemuan hukum).

Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan komparatif (*comparative approach*). Pendekatan perundang-undangan dilakukan dengan mengkaji ketentuan-ketentuan hukum positif yang mengatur tentang perlindungan data pribadi dan kewenangan lembaga negara. Pendekatan konseptual digunakan untuk memahami konsep penemuan hukum, kelembagaan independen, serta prinsip-prinsip hukum yang mendasari pembentukan lembaga perlindungan data pribadi. Sementara itu, pendekatan komparatif dilakukan dengan membandingkan pengaturan dan bentuk kelembagaan perlindungan data pribadi di beberapa negara lain guna memperoleh gambaran ideal yang dapat diterapkan di Indonesia.

Seluruh data yang diperoleh dianalisis menggunakan metode analisis deduktif, yaitu dengan menarik

kesimpulan dari ketentuan umum ke dalam permasalahan yang bersifat khusus (Muhaimin, 2020). Proses analisis ini dimulai dengan pengkajian teori-teori dan asas-asas hukum yang bersifat umum, kemudian diterapkan untuk menjelaskan dan menilai urgensi pembentukan Lembaga PDP di Indonesia sebagai bentuk penemuan hukum yang adaptif terhadap perkembangan era digital.

HASIL DAN PEMBAHASAN

A. Ketidakhadiran Lembaga PDP Sebagai Bentuk Kekosongan Otoritas dalam Rezim PDP

UU PDP secara tegas mengamanatkan pembentukan Lembaga PDP sebagai otoritas independen yang bertanggung jawab dalam penyelenggaraan pelindungan data pribadi di Indonesia. Amanat tersebut tercantum dalam Pasal 58 ayat (2) UU PDP, yang menyatakan bahwa lembaga ini berfungsi melaksanakan perumusan dan penetapan kebijakan, pengawasan, serta penegakan hukum di bidang pelindungan data pribadi. Namun, hingga pertengahan tahun 2025, lembaga tersebut belum juga terbentuk secara resmi. Keterlambatan ini menimbulkan kekosongan otoritas fungsional, khususnya dalam hal pencegahan pelanggaran, pengawasan kepatuhan, dan penyelesaian sengketa yang timbul akibat kebocoran atau penyalahgunaan data pribadi.[2] Akibatnya, fungsi pengawasan sementara ini masih dijalankan oleh Kementerian Komunikasi dan Digitalisasi (untuk selanjutnya disebut "Komdigi"), yang secara kelembagaan bukanlah otoritas independen sebagaimana dimaksud oleh UU PDP.

Situasi ini tentunya menciptakan ketimpangan antara norma dan realitas implementasi, di mana pengaturan hukum sudah tersedia, tetapi organ pelaksana yang seharusnya menjamin efektivitas pelindungan belum beroperasi. Dalam konteks prinsip negara hukum yang demokratis, keterlambatan pembentukan Lembaga PDP dapat dipandang sebagai bentuk ketidakpastian hukum (*legal uncertainty*). Hal ini dikarenakan masyarakat tidak memiliki lembaga rujukan yang jelas untuk menuntut perlindungan atas pelanggaran data pribadi.

Ketiadaan Lembaga PDP bukan sekadar permasalahan administratif, melainkan berimplikasi langsung terhadap efektivitas penegakan hukum dan jaminan perlindungan hak-hak subjek data. Dalam praktiknya, lembaga inilah yang seharusnya menjalankan fungsi regulatif, pengawasan, penegakan, dan penyelesaian sengketa yang timbul akibat pelanggaran terhadap hak subjek data pribadi. Dengan kata lain, lembaga ini bertindak sebagai otoritas independen yang tidak hanya mengawasi, tetapi juga memastikan bahwa setiap pengendali dan prosesor data pribadi melaksanakan prinsip-prinsip pelindungan data sebagaimana ditetapkan oleh hukum. Tanpa Lembaga PDP yang berfungsi penuh dan memiliki legitimasi hukum yang kuat, terdapat risiko bahwa pelaksanaan UU PDP hanya akan berhenti pada tataran normatif, tanpa mampu menghadirkan perlindungan nyata bagi subjek data pribadi. Hal ini pada akhirnya dapat menggerus kepercayaan publik terhadap tata kelola data nasional, serta memperlemah posisi Indonesia dalam ekosistem digital global yang menuntut

[2] Salsa Nabila Hardafi, "Ketiadaan Lembaga PDP: Celah Hukum dalam Pelindungan Data Pribadi", hukumonline, 9 Juli 2025, https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/?page=1

kepatuhan terhadap prinsip-prinsip *data protection* sebagaimana diatur dalam standar internasional seperti *General Data Protection Regulation* di Uni Eropa.

B. Fungsi dan Kewenangan Lembaga PDP di Indonesia

Pada dasarnya, Lembaga PDP merupakan elemen kunci dalam keseluruhan arsitektur penegakan hukum perlindungan data pribadi di Indonesia.[3] Lembaga ini berperan sentral dalam memastikan kepatuhan terhadap standar dan kewajiban PDP oleh para pengendali dan prosesor data pribadi sebagaimana diatur dalam Pasal 59 huruf a UU PDP. Tanpa adanya lembaga yang memiliki otoritas dan independensi kuat, implementasi norma-norma hukum dalam UU PDP akan bersifat parsial dan tidak efektif. Selain itu, Lembaga PDP juga diberi kewenangan untuk merumuskan dan menetapkan kebijakan pelindungan data pribadi yang menjadi pedoman operasional bagi seluruh entitas publik maupun privat sebagaimana diatur dalam Pasal 60 huruf a UU PDP. Fungsi kebijakan ini bersifat strategis dan normatif, karena berfungsi menetapkan arah, standar, serta prinsip nasional dalam tata kelola data pribadi yang aman, transparan, dan akuntabel. Melalui kewenangan tersebut, Lembaga PDP diharapkan menjadi *policy maker* sekaligus *standard setter* dalam memastikan setiap pengendali dan prosesor data pribadi bertindak sesuai dengan prinsip-prinsip dasar pelindungan data.

Merujuk pada ketentuan tersebut, Lembaga PDP dapat merumuskan dan menetapkan kebijakan atau pedoman pengelolaan data pribadi yang lebih operasional, antara lain:

1. Kewajiban bagi perusahaan pengelola data pribadi untuk menunjuk penanggung jawab data pribadi (*Data Protection Officer*/DPO), sebagai pihak yang memastikan kepatuhan internal terhadap regulasi dan prinsip-prinsip pelindungan data pribadi
2. Penerapan standar keamanan data dan manajemen risiko dalam mengelola data pribadi, termasuk standar enkripsi, akses terbatas, serta kebijakan penyimpanan dan pemusnahan data, dan
3. Kewajiban bagi perusahaan untuk memfasilitasi pelatihan atau sertifikasi bagi pengelola data pribadi, guna memastikan kompetensi teknis dan etika dalam pengelolaan data yang sesuai dengan hukum dan prinsip hak asasi manusia.

Kebijakan dan pedoman yang dikeluarkan oleh Lembaga PDP memiliki daya normatif dan administratif yang kuat, sebab menjadi dasar bagi pengendali dan prosesor data pribadi dalam merancang kebijakan internal perusahaan. Dalam konteks ini, Lembaga PDP tidak hanya berperan sebagai pengawas, tetapi juga sebagai otoritas normatif yang mengarahkan bagaimana hukum pelindungan data diimplementasikan secara praktis. Keberadaan lembaga ini diharapkan dapat menciptakan harmonisasi standar nasional pelindungan data pribadi, sekaligus memperkuat kepercayaan publik terhadap tata kelola data di Indonesia. Fungsi penetapan kebijakan oleh Lembaga PDP juga menjadi

[3] Lembaga Studi dan Advokasi Masyarakat (ELSAM), "Lembaga Pelindungan Data Pribadi, Kunci Penegakan Kepatuhan UU PDP", Lembaga Studi dan Advokasi Masyarakat (ELSAM), 17 Oktober 2024, https://www.elsam.or.id/siaran-pers/lembaga-pelindungan-data-pribadi--kunci-penegakan-kepatuhan-uu-pdp, 1 Oktober 2025.

instrumen pencegahan terhadap potensi pelanggaran. Dengan memberikan panduan yang jelas dan terukur, lembaga ini dapat meminimalkan ambiguitas interpretasi hukum yang selama ini sering menjadi celah bagi penyalahgunaan data pribadi oleh korporasi maupun lembaga publik.

Selain kewenangan dalam merumuskan dan menetapkan kebijakan pelindungan data pribadi, berdasarkan Pasal 60 huruf b hingga huruf o, Lembaga PDP juga memegang fungsi pengawasan, penegakan hukum, investigasi dan penyelesaian sengketa, kerja sama lintas negara dan koordinasi kelembagaan, serta transparansi dan akuntabilitas publik, sebagai berikut:

1. Fungsi Pengawasan dan Penegakan Kepatuhan

Lembaga PDP berwenang melakukan pengawasan terhadap kepatuhan Pengendali Data Pribadi dan Prosesor Data Pribadi (huruf b). Kewenangan ini meliputi pelaksanaan audit kepatuhan, pemantauan berkala terhadap sistem manajemen data, serta evaluasi terhadap penerapan prinsip-prinsip pelindungan data. Selain itu, Lembaga PDP juga dapat memberikan perintah tindak lanjut hasil pengawasan (huruf g) kepada pihak yang ditemukan melanggar atau lalai dalam melaksanakan kewajiban hukum. Fungsi ini menjadikan Lembaga PDP sebagai *regulatory watchdog* yang memastikan setiap kegiatan pemrosesan data pribadi dilakukan sesuai asas keabsahan, keadilan, akuntabilitas, dan proporsionalitas sebagaimana diatur dalam Pasal 3 UU PDP.

2. Fungsi Penegakan Hukum Administratif

Dalam konteks penegakan hukum, Lembaga PDP memiliki kewenangan quasi-yudisial untuk menjatuhkan sanksi administratif (huruf c) kepada pengendali atau prosesor data pribadi yang terbukti melakukan pelanggaran. Jenis sanksi tersebut dapat berupa peringatan tertulis, penghentian sementara aktivitas pemrosesan data, penghapusan data pribadi, atau denda administratif sesuai ketentuan Pasal 57 UU PDP. Selain itu, Lembaga PDP juga dapat meminta bantuan hukum kepada Kejaksaan (huruf o) dalam penyelesaian sengketa atau penegakan hasil keputusannya. Kewenangan ini menunjukkan bahwa lembaga tersebut memiliki kapasitas legal untuk memastikan pelaksanaan sanksi dan penegakan hukum administratif secara efektif dan berkekuatan eksekutorial.

3. Fungsi Investigasi, Penelusuran, dan Penyelesaian Sengketa

Kewenangan Lembaga PDP tidak berhenti pada tahap pengawasan, tetapi juga mencakup fungsi investigasi dan penyelidikan administratif. Berdasarkan ketentuan huruf i sampai dengan huruf n, lembaga ini berwenang untuk:

a. Menerima aduan dan laporan masyarakat atas dugaan pelanggaran pelindungan data pribadi
b. Melakukan pemeriksaan, pemanggilan, dan penelusuran terhadap pihak yang diduga melanggar, termasuk pengendali data, badan publik, maupun individu
c. Meminta keterangan, data, dan dokumen sebagai bahan pembuktian
d. Memanggil dan menghadirkan ahli untuk memberikan keterangan teknis maupun hokum, serta
e. Melakukan pemeriksaan terhadap sistem elektronik, sarana, dan tempat yang digunakan oleh pengendali atau prosesor data pribadi.

Sejumlah kewenangan ini menunjukkan bahwa Lembaga PDP memiliki fungsi penyidikan administratif yang bersifat komprehensif, mulai dari tahap deteksi awal, klarifikasi, hingga penetapan keputusan administratif. Mekanisme ini juga memungkinkan lembaga untuk bertindak cepat dalam menangani kasus kebocoran atau penyalahgunaan data pribadi sebelum menimbulkan dampak sistemik yang lebih besar.

4. Fungsi Kerja Sama Internasional dan Koordinasi Penegakan Hukum

Lembaga PDP juga berwenang bekerja sama dengan lembaga pelindungan data pribadi dari negara lain (huruf e), terutama dalam konteks pelanggaran lintas batas (*cross-border data breach*) dan transfer data internasional. Kewenangan ini diperkuat oleh fungsi penilaian terhadap pemenuhan persyaratan transfer data pribadi ke luar wilayah hukum Indonesia (huruf f). Kedua kewenangan tersebut sangat penting dalam era globalisasi digital, mengingat banyaknya perusahaan multinasional dan penyedia layanan berbasis cloud yang beroperasi lintas yurisdiksi. Lembaga PDP berperan untuk memastikan bahwa setiap transfer data internasional mematuhi prinsip *adequacy*, *safeguard*, dan *consent*, sebagaimana praktik yang diterapkan di Uni Eropa melalui GDPR.

5. Fungsi Transparansi dan Akuntabilitas Publik

Lembaga PDP memiliki kewenangan untuk melakukan publikasi hasil pelaksanaan pengawasan pelindungan data pribadi (huruf h). Publikasi ini berfungsi sebagai bentuk transparansi dan pertanggungjawaban publik, sekaligus sebagai mekanisme naming and shaming terhadap pihak yang melanggar. Dengan begitu, lembaga ini turut berkontribusi menciptakan budaya kepatuhan dan meningkatkan kesadaran masyarakat terhadap pentingnya pelindungan data pribadi.

C. Komparasi Pengaturan, Prinsip, dan Model Lembaga PDP di Malaysia, Singapura, Hongkong, dan Jepang

1. Malaysia

Malaysia merupakan salah satu negara di kawasan Asia Tenggara yang telah memiliki regulasi komprehensif dalam bidang perlindungan data pribadi melalui *Personal Data Protection Act* yang disahkan pada tahun 2010. Regulasi ini menjadi tonggak penting dalam menjamin keamanan dan privasi informasi individu, terutama dalam konteks transaksi komersial dan aktivitas ekonomi digital yang melibatkan pertukaran data secara luas. *Personal Data Protection Act* Malaysia mengatur secara jelas mengenai pengumpulan, penyimpanan, pemrosesan, serta transfer data pribadi oleh pihak yang disebut sebagai data *user*, dengan tujuan utama untuk melindungi kepentingan hukum dan hak-hak subjek data (*data subject*).

Pelaksanaan *Personal Data Protection Act* diawasi oleh lembaga otoritatif bernama Pesuruhjaya Perlindungan Data Peribadi, yang secara struktural bertanggung jawab kepada Menteri Komunikasi dan Multimedia Malaysia. Lembaga ini berfungsi sebagai pengawas utama dalam penerapan prinsip-prinsip perlindungan data pribadi, sekaligus berperan dalam penegakan hukum terhadap pelanggaran yang dilakukan oleh pihak pengendali atau pemroses data. Keberadaan lembaga tersebut merupakan bentuk komitmen pemerintah Malaysia dalam membangun sistem perlindungan data yang kuat, transparan, dan akuntabel.

Substansi utama *Personal Data Protection Act* Malaysia berlandaskan pada prinsip *consent-based protection*, yakni bahwa setiap pengumpulan dan pemrosesan data pribadi harus

dilakukan berdasarkan persetujuan eksplisit dari individu yang bersangkutan. Persetujuan ini merupakan wujud pengakuan atas hak kendali individu terhadap data pribadinya, serta menjadi dasar legitimasi hukum bagi setiap tindakan pemrosesan data. Selain itu, pengendali data diwajibkan memberikan informasi yang jelas dan terbuka mengenai tujuan pengumpulan data, jangka waktu penyimpanan, serta pihak-pihak yang akan menerima data tersebut. Melalui mekanisme ini, individu juga diberikan hak untuk mengakses, memperbarui, memperbaiki, atau bahkan membatasi penggunaan data pribadinya sesuai dengan ketentuan yang berlaku.

Personal Data Protection Act Malaysia juga menegaskan pentingnya penerapan prinsip-prinsip legalitas, kebutuhan, dan proporsionalitas dalam pengelolaan data pribadi. Setiap pemrosesan data harus dilakukan secara sah dan tidak boleh melampaui tujuan yang telah ditetapkan pada saat pengumpulan. Pengendali data juga diwajibkan menjaga integritas, kerahasiaan, dan keamanan data pribadi agar tidak terjadi kebocoran, penyalahgunaan, atau akses tidak sah yang dapat merugikan individu.

Terkait dengan transfer data pribadi lintas negara, *Personal Data Protection Act* Malaysia menerapkan pembatasan yang ketat. Pasal-pasal dalam undang-undang ini menyatakan bahwa data pribadi tidak boleh ditransfer ke luar wilayah Malaysia, kecuali apabila negara tujuan telah memenuhi tingkat perlindungan data yang sebanding atau lebih tinggi dibandingkan dengan standar *Personal Data Protection Act* Malaysia. Transfer lintas negara hanya dapat dilakukan dengan izin dan penetapan resmi dari Menteri Penerangan, Kebudayaan, dan Komunikasi. Ketentuan ini bertujuan untuk memastikan bahwa perlindungan terhadap data pribadi warga negara Malaysia tetap terjaga, bahkan ketika data tersebut berpindah ke yurisdiksi asing (Matheus & Gunadi, 2024).

Melalui kerangka hukum yang kokoh serta keberadaan lembaga pengawas yang memiliki otoritas penuh, Malaysia telah menunjukkan keseriusannya dalam membangun rezim perlindungan data pribadi yang sejalan dengan praktik terbaik internasional. Model *Personal Data Protection Act* Malaysia dapat menjadi referensi berharga bagi Indonesia dalam membangun Lembaga PDP yang independen dan efektif, guna memastikan kepatuhan terhadap prinsip-prinsip hukum data modern serta menjamin perlindungan hak-hak privasi warga negara di era digita.

2. Singapura

Singapura telah menjadi salah satu negara di kawasan Asia Tenggara yang memiliki regulasi komprehensif mengenai perlindungan data pribadi melalui *Personal Data Protection Act* yang diberlakukan sejak tahun 2012. Undang-undang ini mengatur secara rinci mengenai mekanisme pengumpulan (*acquisition*), penggunaan (*use*), dan pengungkapan (*disclosure*) data pribadi oleh individu, badan usaha, maupun lembaga publik di Singapura. *Personal Data Protection Act* hadir sebagai instrumen hukum untuk menyeimbangkan antara kebutuhan dunia usaha dalam memanfaatkan data pribadi untuk kepentingan komersial, dengan perlindungan atas hak privasi individu warga negara.

Pelaksanaan dan pengawasan terhadap *Personal Data Protection Act* berada di bawah tanggung jawab *Personal Data Protection Commission,* yakni lembaga otoritatif yang berada di bawah koordinasi Menteri Komunikasi dan Informasi Singapura. *Personal Data Protection Commission* berperan tidak

hanya sebagai pengawas, tetapi juga sebagai pembuat kebijakan dan pedoman operasional yang menjadi acuan bagi seluruh pelaku usaha dan organisasi yang memproses data pribadi. Melalui penerbitan berbagai panduan teknis dan *advisory guidelines*, *Personal Data Protection Commission* memastikan bahwa setiap pengendali data memahami kewajibannya untuk bertindak secara transparan, adil, dan bertanggung jawab dalam setiap tahapan pengelolaan data pribadi.

Salah satu prinsip utama dalam *Personal Data Protection Act* adalah kewajiban untuk memperoleh persetujuan eksplisit dari individu sebelum data pribadinya dikumpulkan, digunakan, atau diungkapkan. Prinsip ini menegaskan hak kendali (*control rights*) yang melekat pada setiap individu atas informasi pribadinya, sekaligus menjadi fondasi bagi kepercayaan publik terhadap sistem perlindungan data nasional. Selain itu, *Personal Data Protection Act* juga mengatur mekanisme *cross-border data transfer* yang ketat. Setiap organisasi yang hendak mentransfer data pribadi ke luar negeri wajib memastikan bahwa negara atau entitas penerima data tersebut memiliki tingkat perlindungan yang setara dengan standar yang berlaku di Singapura. Ketentuan ini mencerminkan komitmen pemerintah Singapura untuk menjaga keamanan data pribadi warganya, bahkan ketika data tersebut berada di luar yurisdiksi nasional.

Dalam hal penegakan hukum, *Personal Data Protection Commission* memiliki kewenangan luas untuk melakukan investigasi, memerintahkan tindakan korektif, serta menjatuhkan sanksi administratif terhadap organisasi yang terbukti melanggar ketentuan *Personal Data Protection Act*. Pelanggaran terhadap regulasi ini dapat dikenai denda dalam jumlah besar, dengan batas maksimum mencapai SGD 1 juta, tergantung pada tingkat keseriusan dan dampak pelanggaran yang terjadi. Penerapan sanksi yang tegas ini menunjukkan bahwa Singapura menempatkan isu perlindungan data pribadi sebagai bagian integral dari tata kelola pemerintahan yang bersih, transparan, dan berbasis kepercayaan publik (Ayiliani & Farida, 2024).

3. Hongkong

Hong Kong merupakan negara pertama di kawasan Asia yang menetapkan kerangka regulatif komprehensif untuk perlindungan data pribadi, melalui *Personal Data (Privacy) Ordinance* (untuk selanjutnya "PDPO") yang diberlakukan pada tahun 1995 dan kemudian mengalami perubahan signifikan pada tahun 2012. Regulasi ini menjadi tonggak penting dalam pengembangan tata kelola data pribadi di Asia karena memperkenalkan prinsip-prinsip dasar data protection yang sejalan dengan praktik terbaik global.

Pelaksanaan PDPO berada di bawah pengawasan lembaga independen bernama *Privacy Commissioner for Personal Data* (untuk selanjutnya "PCPD"). PCPD berperan sebagai otoritas pengatur dan pengawas pelindungan data pribadi yang memiliki tanggung jawab langsung kepada *Chief Executive* Hong Kong. Meskipun secara administratif PCPD berada di bawah struktur pemerintahan, lembaga ini diberikan otonomi fungsional yang luas untuk menjamin independensi dalam melaksanakan tugas pengawasan, investigasi, dan penegakan hukum terhadap pelanggaran privasi data.

Prinsip perlindungan hak privasi yang diatur dalam PDPO mencakup beberapa aspek mendasar, antara lain:

a. Prinsip tujuan yang sah (*Purpose Specification Principle*) — pengumpulan data pribadi harus dilakukan dengan tujuan yang sah dan relevan dengan kepentingan pengumpul

b. Prinsip pembatasan penggunaan (*Use Limitation Principle*) — penggunaan dan pengungkapan data pribadi hanya boleh dilakukan sesuai dengan tujuan awal pengumpulan, kecuali atas dasar persetujuan eksplisit dari pemilik data (*data subject consent*)
c. Prinsip akurasi dan ketepatan waktu (*Data Accuracy and Retention Principle*) — data pribadi harus akurat, lengkap, dan diperbarui secara berkala serta hanya disimpan selama diperlukan
d. Prinsip keamanan data (*Data Security Principle*) — pengendali data wajib melindungi data pribadi dari akses, pemrosesan, atau pengungkapan yang tidak sah, dan
e. Prinsip keterbukaan (*Openness and Transparency Principle*) — pengendali data diwajibkan untuk menyediakan informasi yang jelas tentang kebijakan privasi dan tujuan penggunaan data, termasuk apabila data tersebut dikelola oleh pihak ketiga.

Pelanggaran terhadap ketentuan PDPO dapat menimbulkan konsekuensi hukum yang serius. PCPD memiliki kewenangan untuk melakukan *formal investigation*, mengeluarkan *enforcement notice* atau somasi resmi, serta merekomendasikan tindakan hukum terhadap entitas yang terbukti melanggar. Model penegakan hukum ini memperlihatkan keseimbangan antara fungsi pengawasan administratif dan perlindungan hak individu, di mana fokusnya tidak hanya pada penindakan tetapi juga pada edukasi dan pembinaan kepatuhan terhadap standar privasi data. Dari sudut pandang komparatif, struktur PCPD dapat menjadi model kelembagaan ideal bagi Lembaga PDP di Indonesia, karena mencerminkan prinsip independensi fungsional sebagaimana dianut dalam GDPR. PCPD berfungsi tidak sekadar sebagai lembaga administratif, melainkan sebagai institusi yang menjamin accountability pengendali data dan *transparency* dalam pengelolaan informasi pribadi publik (Tsamara, 2021).

4. Jepang

Jepang telah memiliki regulasi komprehensif terkait perlindungan data pribadi melalui *Act on the Protection of Personal Information* yang diberlakukan sejak tahun 2003. Regulasi ini menjadi dasar hukum utama bagi seluruh aktivitas pengumpulan, penyimpanan, pemrosesan, dan transfer data pribadi di Jepang, baik oleh lembaga publik maupun sektor swasta. Pengawasan atas implementasi *Act on the Protection of Personal Information* dilakukan oleh sebuah lembaga administratif independen bernama *Personal Information Protection Commission*, yang bertanggung jawab langsung kepada Parlemen Jepang. Kemandirian *Personal Information Protection Commission* dimaksudkan agar pelaksanaan fungsi pengawasan tidak terpengaruh oleh kepentingan politik maupun korporasi, sekaligus memastikan penerapan prinsip-prinsip perlindungan data yang berkeadilan, transparan, dan akuntabel di seluruh wilayah yurisdiksi Jepang.

Amandemen *Act on the Protection of Personal Information* pada tahun 2020 menjadi tonggak penting dalam memperkuat tata kelola data pribadi, khususnya dalam konteks globalisasi arus informasi dan perdagangan digital lintas negara. Perubahan ini memperkenalkan ketentuan baru mengenai *cross-border*

data transfer, yakni transfer data pribadi ke luar wilayah Jepang. Berdasarkan ketentuan tersebut, setiap perusahaan yang berada di bawah yurisdiksi hukum Jepang wajib memperoleh persetujuan eksplisit dari individu pemilik data sebelum melakukan transfer data pribadi mereka ke negara lain. Lebih lanjut, *Act on the Protection of Personal Information* mengharuskan perusahaan pengekspor data untuk membuat perjanjian tertulis dengan entitas penerima di luar negeri. Kontrak ini harus memuat komitmen kedua belah pihak untuk menerapkan standar keamanan dan perlindungan data yang setara dengan yang diatur dalam *Act on the Protection of Personal Information*. Kewajiban hukum tersebut tidak hanya berhenti pada entitas penerima pertama. Dalam hal informasi pribadi tersebut kembali dialihkan atau ditransfer kepada pihak ketiga di negara lain, pengendali data asal memiliki tanggung jawab penuh untuk memastikan bahwa seluruh pihak penerima berikutnya tetap mematuhi standar keamanan dan perlindungan data yang sama.

Terkait penegakan hukumnya, Jepang menerapkan sistem sanksi yang tegas terhadap pelanggaran *Act on the Protection of Personal Information*. Pelaku pelanggaran, baik individu maupun korporasi, dapat dikenai denda dalam jumlah signifikan, perintah administratif dari *Personal Information Protection Commission*, hingga sanksi pidana apabila pelanggaran tersebut menimbulkan dampak serius terhadap privasi individu. Pendekatan hukum Jepang melalui *Act on the Protection of Personal Information* menekankan keseimbangan antara kemajuan ekonomi digital dan perlindungan hak asasi individu atas data pribadinya. Model regulasi dan kelembagaan seperti *Personal Information Protection Commission* ini dapat menjadi acuan bagi Indonesia dalam membangun Lembaga Perlindungan Data Pribadi yang benar-benar independen dan efektif, guna menjamin kepastian hukum dan kepercayaan publik dalam tata kelola data di era digital.

D. Formulasi Desain Lembaga PDP yang Ideal

Lembaga PDP yang ideal bagi Indonesia seyogianya dibentuk dengan mengacu pada prinsip independensi institusional sebagaimana diatur dalam GDPR, yang menempatkan otoritas pelindungan data sebagai entitas negara yang bebas dari intervensi kekuasaan eksekutif maupun kepentingan politik. Independensi ini bukan semata-mata simbolik, melainkan merupakan prasyarat normatif agar lembaga tersebut dapat menjalankan fungsi pengawasan dan penegakan hukum secara objektif, transparan, dan berkeadilan. Oleh karena itu, keanggotaan lembaga idealnya berasal dari unsur non-pemerintah—seperti pakar hukum, akademisi, praktisi teknologi informasi, serta tokoh masyarakat yang memiliki integritas tinggi—namun secara kelembagaan tetap memperoleh legitimasi konstitusional dan pembiayaan dari anggaran negara.

Dalam desain kelembagaan seperti ini, Lembaga PDP berfungsi sebagai otoritas independen negara yang tidak tunduk secara hierarkis kepada kementerian atau lembaga manapun, melainkan bertanggung jawab langsung kepada publik melalui mekanisme akuntabilitas yang diatur dalam undang-undang. Konsep ini meniru model *Data Protection Authority* (untuk selanjutnya disebut "DPA") di Uni Eropa yang memiliki kewenangan penuh untuk mengawasi kepatuhan, menjatuhkan sanksi administratif, serta memberikan rekomendasi kebijakan tanpa tekanan politik sehingga independensi bukan hanya dilihat dari aspek struktural, tetapi juga dari jaminan kebebasan dalam pengambilan keputusan,

mekanisme pengawasan yang transparan, dan sistem penganggaran yang terpisah dari lembaga eksekutif.

Realisasi keberadaan lembaga semacam ini di Indonesia memiliki arti strategis dalam menjamin efektivitas pelaksanaan UU PDP. Tanpa lembaga yang benar-benar independen, fungsi pengawasan dan penegakan hukum terhadap pelanggaran data pribadi berisiko tidak berjalan optimal karena adanya potensi konflik kepentingan, terutama ketika entitas yang diawasi adalah lembaga pemerintahan itu sendiri (Matheus & Gunadi, 2024). Oleh sebab itu, pembentukan Lembaga Pengawas Pelindungan Data Pribadi yang bersifat independen menjadi keharusan konstitusional sekaligus manifestasi komitmen negara terhadap pemenuhan hak privasi dan hak atas rasa aman digital warga negara. Lembaga ini nantinya akan menjadi garda terdepan dalam memastikan kepatuhan para pengendali dan prosesor data pribadi, baik yang berasal dari individu, badan publik, maupun korporasi swasta. Selain mengawasi kepatuhan, lembaga tersebut juga berperan dalam memberikan edukasi publik, menyusun kebijakan nasional pelindungan data, serta menjadi mediator dalam sengketa antara subjek data dan pengendali data pribadi.

Lembaga Pengawas Data Pribadi pada dasarnya dapat dibentuk berdasarkan konsep *Independent Regulatory Agencies*. Konsep *Independent Regulatory Agencies*, sebagaimana dikemukakan oleh Rizki Ramadani, menjelaskan bahwa lembaga independen memiliki dua bentuk utama dari sisi kemandiriannya, yakni independensi formal dan independensi *de facto* (Ramadani, 2020). Independensi formal mengacu pada jaminan hukum yang tertuang dalam peraturan perundang-undangan, yang meliputi tiga dimensi: independensi personalia, yaitu kebebasan dalam pengangkatan dan pemberhentian pejabat tanpa intervensi politik; independensi fungsional, yakni otonomi dalam pelaksanaan fungsi dan kewenangan tanpa tekanan dari lembaga lain; serta independensi institusional, yang berarti lembaga tersebut berdiri sendiri di luar hierarki kekuasaan eksekutif, legislatif, maupun yudikatif. Sementara itu, independensi de facto merujuk pada kondisi aktual dalam praktik penyelenggaraan kewenangan lembaga tersebut, di mana lembaga benar-benar bebas dari pengaruh pihak manapun dalam mengambil keputusan dan menjalankan tugasnya. Dengan kata lain, aspek ini menilai sejauh mana independensi formal yang dijamin secara hukum benar-benar diimplementasikan dalam tataran praktis.

Terdapat tiga aspek utama dalam konsep *Independent Regulatory Authorities*, yakni: pertama, independensi dari pejabat-pejabat terpilih, yang berarti lembaga tidak boleh menjadi alat kekuasaan pemerintah atau partai politik tertentu; kedua, interaksi yang seimbang dengan lembaga administratif lain, di mana lembaga tetap menjalin koordinasi tanpa kehilangan otonominya; dan ketiga, mekanisme pengambilan keputusan yang transparan, akuntabel, dan berbasis profesionalitas. Model kelembagaan seperti ini telah diterapkan pada beberapa lembaga independen di Indonesia, antara lain Komisi Pemilihan Umum yang berwenang menyelenggarakan pemilu secara mandiri, Otoritas Jasa Keuangan yang mengawasi sektor keuangan secara terpisah dari pemerintah, serta Ombudsman Republik Indonesia yang bertugas mengawasi pelayanan publik. Oleh karena itu, pembentukan Lembaga Pengawas Data Pribadi yang berlandaskan pada konsep IRAs menjadi sangat relevan untuk menjamin bahwa pelindungan data pribadi di Indonesia tidak hanya bersifat administratif, tetapi

juga memiliki kekuatan kelembagaan yang independen dan efektif dalam menegakkan kepatuhan, memberikan sanksi, serta menjaga hak-hak subjek data dari intervensi kepentingan politik maupun ekonomi.

Konsep *Independent Regulatory Agencies* dipandang mampu menciptakan keseimbangan peran antara sektor administrasi publik, organisasi masyarakat sipil, dan warga negara. *Independent Regulatory Agencies* dirancang bukan sekadar sebagai pelaksana fungsi administratif, tetapi sebagai lembaga pengatur yang berdiri di atas kepentingan politik dan ekonomi, serta berperan sebagai penengah antara negara, pelaku usaha, dan masyarakat. Dalam konteks pelindungan data pribadi, keberadaan lembaga dengan karakteristik semacam ini menjadi sangat penting untuk menjamin agar kepentingan publik tidak tereduksi oleh kepentingan institusional maupun korporasi yang memiliki kekuatan ekonomi besar. Melalui penerapan konsep *Independent Regulatory Agencies*, Lembaga PDP idealnya memiliki kewenangan yang berdiri sendiri, baik secara struktural maupun fungsional. Artinya, lembaga tersebut tidak berada di bawah subordinasi kementerian atau lembaga eksekutif lainnya, sehingga keputusan dan kebijakannya bebas dari intervensi politik maupun tekanan birokratis. Pemisahan kelembagaan ini dimaksudkan untuk meminimalisasi potensi konflik kepentingan dan meningkatkan kredibilitas pengawasan, terutama dalam penegakan hukum terkait pelindungan data pribadi.

Urgensi pembentukan lembaga independen semakin menguat mengingat arus transfer data pribadi lintas negara (*cross-border data transfer*) yang semakin masif di era ekonomi digital global. Data pribadi kini menjadi komoditas bernilai ekonomi tinggi, yang menuntut adanya mekanisme pengawasan yang tidak hanya bersifat nasional, tetapi juga responsif terhadap standar dan praktik internasional seperti GDPR di Uni Eropa. Oleh sebab itu, lembaga pengawas yang berlandaskan prinsip *Independent Regulatory Agencies* akan memiliki posisi strategis dalam mengatur, mengawasi, serta menjatuhkan sanksi atas pelanggaran pelindungan data pribadi, baik oleh entitas domestik maupun asing, tanpa campur tangan politik atau tekanan ekonomi.

SIMPULAN

Ketiadaan Lembaga PDP pasca disahkannya UU PDP telah menimbulkan kekosongan otoritas yang berdampak langsung terhadap efektivitas penerapan norma hukum dalam bidang perlindungan data pribadi. Tanpa adanya lembaga khusus yang independen, prinsip-prinsip perlindungan data sebagaimana dimandatkan oleh undang-undang tidak dapat dijalankan secara optimal. Pengawasan yang untuk sementara berada di bawah kewenangan Komdigi cenderung problematis karena menimbulkan potensi konflik kepentingan, terutama mengingat posisi Komdigi sebagai salah satu data controller di sektor publik. Kondisi ini berimplikasi pada lemahnya independensi dan akuntabilitas dalam proses pengawasan dan penegakan hukum terhadap pelanggaran data pribadi.

Oleh sebab itu, pembentukan Lembaga PDP yang bersifat independen, otonom, serta bebas dari intervensi politik merupakan kebutuhan hukum yang mendesak. Lembaga ini diperlukan agar pelaksanaan UU PDP tidak berhenti pada tataran normatif, melainkan dapat berjalan secara operasional dan efektif dalam menjamin perlindungan hak konstitusional warga negara atas privasi. Hasil kajian perbandingan dengan negara-negara seperti Malaysia, Singapura, Hong Kong, dan Jepang menunjukkan bahwa model *Independent*

Regulatory Agencies terbukti paling ideal untuk diterapkan di Indonesia. Lembaga dengan model tersebut memiliki independensi baik secara formal maupun *de facto*, dengan fungsi utama mencakup pengawasan terhadap kepatuhan, investigasi atas dugaan pelanggaran, penerapan sanksi administratif, penyelesaian sengketa, serta koordinasi internasional dalam hal transfer data lintas batas negara. Keberadaan Lembaga PDP akan menjadi instrumen kunci dalam mewujudkan keadilan, kepastian hukum, serta kemanfaatan bagi masyarakat dalam tata kelola data pribadi di era digital yang semakin kompleks.

Selain itu, Lembaga PDP perlu dibekali dengan kewenangan quasi-yudisial agar dapat menjatuhkan sanksi administratif, memerintahkan tindakan korektif, serta menyelesaikan sengketa pelanggaran data pribadi secara efektif dan berkeadilan. Di sisi lain, pemerintah bersama DPR juga perlu melakukan harmonisasi regulasi antara UU PDP, UU ITE, serta instrumen hukum internasional terkait transfer data lintas negara, agar mekanisme perlindungan data pribadi di Indonesia sejalan dengan prinsip *adequacy* dan *consent-based protection* yang diakui secara global. Terakhir, penguatan kapasitas sumber daya manusia serta peningkatan literasi publik mengenai pelindungan data pribadi harus menjadi agenda prioritas nasional. Upaya ini penting agar pelaksanaan UU PDP dan keberadaan lembaga pelaksananya dapat benar-benar berfungsi sebagai pilar utama dalam membangun budaya hukum perlindungan data yang kuat, adaptif, dan berorientasi pada hak asasi manusia di era digital.

Penulis menyarankan agar Pemerintah segera merealisasikan pembentukan Lembaga PDP sebagaimana diperintahkan secara eksplisit dalam Pasal 58 ayat (2) UU PDP. Pembentukan lembaga ini harus dilaksanakan dengan menjamin adanya independensi struktural, fungsional, dan institusional yang diakui serta dilindungi secara hukum. Untuk mewujudkannya, diperlukan penyusunan peraturan turunan dalam bentuk Peraturan Pemerintah atau Peraturan Presiden yang bersifat komprehensif, terukur, dan implementatif. Regulasi tersebut harus memuat pengaturan secara rinci mengenai mekanisme rekrutmen pimpinan dan anggota lembaga, struktur organisasi, pembagian kewenangan, tata kelola internal, serta sumber pembiayaan lembaga. Kejelasan dan ketegasan pengaturan tersebut menjadi krusial untuk menjamin prinsip transparansi, akuntabilitas, efisiensi, dan keberlanjutan kelembagaan, sehingga Lembaga PDP dapat berfungsi secara optimal sebagai otoritas yang independen dalam menegakkan prinsip-prinsip pelindungan data pribadi di Indonesia.

DAFTAR PUSTAKA

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, *6*(3), 431–455.

Dewi, S. (2016). Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia. *Yustisia Jurnal Hukum*, *5*(1). https://doi.org/10.20961/yustisia.v5i1.8712

Lie, G., Redi, A., & Ramadhan, D. A. (2022). Komisi Independen Perlindungan Data Pribadi: Quasi Peradilan Dan Upaya Terciptanya Right To Be Forgotten Di Indonesia Kajian Putusan Nomor 438/Pid.Sus/2020/PN JKT.UTR. *Jurnal Yudisial*, *15*(2), 227–246. https://doi.org/10.29123/jy.v15i2.530.

Marzuki, P. M. (2019). *Penelitian Hukum: Edisi Revisi* (19th ed.). Prenada Media Group.

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *JUSTISI*, *10*(1), 20–35.

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.

Pohan, T. D., & Nasution, M. I. P. (2023). PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN DALAM PLATFORM E COMMERCE. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, *1*(3), 42–48. https://doi.org/10.47861/sammajiva.v1i3.336

Ramadani, R. (2020). Lembaga Negara Independen Di Indonesia Dalam Perspektif Konsep Independent Regulatory Agencies. *Jurnal Hukum Ius Quia Iustum*, *27*(1). https://doi.org/10.20885/iustum.vol27.iss1.art9

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53. https://doi.org/10.26740/jsh.v3n1.p53-84