NOMOKRASI
JURNAL LeDHaK FAKULTAS HUKUM UNHAS
Volume 2 Nomor 2 Tahun 2024

GAGASAN PELINDUNGAN DATA PRIBADI OLEH LPPDP INDONESIA: SEBUAH STUDI PERBANDINGAN DENGAN OTORITAS PELINDUNGAN DATA PRIBADI SINGAPURA

Muhammad Fadel Adhyputra[1], Thoriq Ahmadi[2], Mohammad Rifqi[3]
[123]*Fakultas Syariah dan Hukum, Universitas Islam Negeri Sunan Kalijaga Yogyakarta*

Article Info

Corresponding Author:
Penulis Korespondensi
✉fadeladhyputra@gmail.com

Keyword:
Cyber Law; Digital Governance; Personal data protection

Kata Kunci:
Hukum Siber; Pelindungan data pribadi; Tata Kelola Digital

Abstract

This research aims to design an ideal Personal Data Protection Implementing Agency (LPPDP) model for Indonesia, by referring to the best practices of data protection agencies in other countries, particularly Singapore. Increasing digital activities and cyberattacks, especially in the government sector, have highlighted the urgency of personal data protection in Indonesia. Although the Law on Personal Data Protection has been passed, the absence of LPPDP as an independent oversight institution is an obstacle to data protection law enforcement and supervision. Through a normative and comparative legal approach, this research compares the design of LPPDP with the Personal Data Protection Commission (PDPC) and Smart Nation and Digital Government Group (SNDGG) in Singapore. The results show that LPPDP needs to be established as an independent institution with strong authority in law enforcement and comprehensive supervision. The PDPC and SNDGG models can be a reference in establishing an effective institution in Indonesia. Thus, the establishment of LPPDP is expected to improve personal data protection, provide legal certainty, and build public trust in data governance in Indonesia.

Abstrak

Penelitian ini bertujuan untuk merancang model Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) yang ideal bagi Indonesia, dengan merujuk pada praktik terbaik lembaga perlindungan data di negara lain, khususnya Singapura. Meningkatnya aktivitas digital dan serangan siber, telah menyoroti urgensi perlindungan data pribadi di Indonesia. Meskipun Undang-Undang Pelindungan Data Pribadi telah disahkan, absennya LPPDP sebagai lembaga pengawas yang independen menjadi kendala dalam penegakan hukum dan pengawasan perlindungan data. Melalui penelitian hukum normatif dengan pendekatan komparatif dan peraturan perundang-undangan, penelitian ini membandingkan rancangan LPPDP dengan Personal Data Protection Commission (PDPC) dan Smart Nation and Digital Government Group (SNDGG) di Singapura. Hasil penelitian menunjukkan bahwa LPPDP perlu dibentuk sebagai lembaga independen dengan kewenangan yang kuat dalam penegakan hukum dan pengawasan menyeluruh. Model PDPC dan SNDGG dapat menjadi acuan dalam membentuk lembaga yang efektif di Indonesia. Dengan demikian, pembentukan LPPDP diharapkan dapat meningkatkan pelindungan data pribadi, memberikan kepastian hukum, dan membangun kepercayaan publik terhadap tata kelola data di Indonesia.

1. PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mengubah tatanan kehidupan masyarakat modern. Penggunaan internet dan platform digital dalam berbagai aspek kehidupan telah menjadi bagian yang tidak terpisahkan. Namun, di balik kemudahan yang ditawarkan, terdapat tantangan serius terkait pelindungan data pribadi. Meningkatnya aktivitas *online* telah memicu peningkatan kasus pelanggaran data, di mana informasi pribadi individu dapat dengan mudah diakses, disalahgunakan, atau diperdagangkan tanpa izin. Absennya lembaga yang bertanggung jawab atas pelindungan data pribadi telah menjadi kendala utama dalam upaya melindungi data pribadi di Indonesia. Hal ini terbukti dengan meningkatnya kasus kebocoran data yang melibatkan berbagai sektor, termasuk sektor pemerintahan. Tanpa adanya lembaga pengawas yang kuat, pelaku pelanggaran data sulit untuk dimintai pertanggungjawaban secara hukum, sehingga menimbulkan rasa tidak aman di kalangan masyarakat. Maka dari itu, diperlukan pembentukan Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) sebagai otoritas untuk melindungi dan menegakkan hukum atas pelanggaran data pribadi di Indonesia.

Kasus kebocoran data di Indonesia terus meningkat signifikan. Badan Siber dan Sandi Negara (BSSN) mencatat 149 kasus dugaan kebocoran data hingga Juni 2024, sementara pada 2022 tercatat 311 kasus. Sebagian besar kasus melibatkan penyelenggara sistem elektronik (PSE) swasta dan pemerintah, tetapi sanksi yang dijatuhkan masih terbatas pada teguran dan rekomendasi, mengingat lembaga pelindungan data belum terbentuk.[1] Beberapa negara, seperti Singapura, telah lebih dulu membentuk lembaga pelindungan data yang efektif, yaitu Personal Data Protection Commission (PDPC) dan Smart Nation and Digital Government Group (SNDGG), yang mengatur mekanisme pelindungan data serta penegakan hukum pelanggaran privasi. Seiring dengan konsep pembangunan *smart city* di Ibu Kota Nusantara (IKN) yang mengandalkan teknologi digital, urgensi pembentukan LPPDP semakin mendesak. *Smart city* membutuhkan pengelolaan data pribadi yang masif, sehingga lembaga pengawas yang kuat diperlukan untuk memastikan keamanan data. Tanpa lembaga khusus, risiko kebocoran data di IKN dapat berdampak serius pada keamanan publik dan pemerintahan.[2]

Pasal 28G ayat 1 UUD 1945 berbunyi bahwasanya Setiap orang berhak atas perlindungan 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.[3] Pasal ini memberikan landasan konstitusional yang kuat bagi pelindungan data pribadi, meskipun tidak disebutkan secara eksplisit. Meningkatnya aktivitas masyarakat dalam bertransaksi

[1] Imail et al., *Keamanan Data Pribadi Terkait Penyelenggaraan Pemilu* (Jakarta: TEMPO Publishing, 2024), hlm. 14.

[2] Kominfo, "Keamanan Siber Jadi Kunci Membangun Kota Cerdas IKN," *Kominfo.Go.Id*, November 3, 2023, https://www.kominfo.go.id/content/detail/52710/keamanan-siber-jadi-kunci-membangun-kota-cerdas-ikn/0/berita.

[3] Undang-Undang Dasar Republik Indonesia Tahun 1945 Pasal 28G Ayat 1.

online menjadikan kerentanan terhadap penyalahgunaan data pribadi serta pelanggaran privasi.[4] Pemerintah Indonesia telah merespon ancaman ini dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada September 2022, yang di dalamnya juga mengatur pembentukan Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP). Namun, meskipun undang-undang tersebut sudah diberlakukan, lembaga yang seharusnya mengawasi dan memastikan keamanan data tersebut hingga kini belum terbentuk.[5]

Berdasarkan berbagai literatur terkait, perlindungan data pribadi di Indonesia masih menghadapi berbagai tantangan, termasuk absennya lembaga pengawas yang mandiri. Widjaja & Cesarianti (2020) menekankan urgensi pembentukan LPPDP untuk mengawasi pelanggaran data.[6] Faizah et al. (2023) membandingkan regulasi Indonesia dengan Singapura dan Hong Kong, serta menyoroti efektivitas lembaga pengawas independen seperti PDPC dalam memperkuat perlindungan data pribadi.[7] Arthaputri et al. (2022) menyebut bahwa UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia perlu didukung lembaga pengawas agar sejalan dengan standar internasional.[8] Halbert et al. (2023) menambahkan bahwa harmonisasi hukum dengan negara lain seperti Jepang dan Singapura dapat menjadi acuan bagi Indonesia dalam membentuk otoritas pelindung data yang independen.[9] Berdasarkan perbandingan internasional, pembentukan lembaga ini sangat penting untuk meningkatkan efektivitas penegakan hukum dan menjaga kepercayaan publik terhadap keamanan data di Indonesia.

Oleh karena itu, fokus penelitian ini adalah analisis komparatif antara rancangan Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) di Indonesia dan lembaga pelindungan data internasional. Hal tersebut diperlukan untuk memahami sejauh mana kesenjangan yang ada dalam pelindungan data pribadi. Dalam penelitian ini, perbandingan akan diarahkan pada lembaga pelindungan data di Singapura, mengingat

[4] Giovanno Halbert et al, "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia," *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, no. 3 (December 21, 2023), hlm. 307, https://doi.org/10.55809/tora.v9i3.275.

[5] Azza Fitrahul Faizah et al., "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," *Hakim: Jurnal Ilmu Hukum dan Sosial* 1, no. 3 (2023), hlm.7 , https://doi.org/10.51903/hakim.v1i3.1222.

[6] Gunawan Widjaja and Fransiska Milenia Cesarianti, "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 dan Pasal 60 Undang–Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (April 24, 2024), hlm. 241, https://doi.org/10.62335/8qf44b59.

[7] Azza Fitrahul Faizah et al., "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," *Hakim: Jurnal Ilmu Hukum dan Sosial* 1, no. 3 (2023), hlm. 24, https://doi.org/10.51903/hakim.v1i3.1222.

[8] Sylvia Faradina Amandasari Arthaputri, Ahmad Syaifudin, and M Fahrudin, "Perlindungan Data Pribadi sebagai Bentuk Perwujudan Cyber Security (Studi Komparatif Indonesia dan Singapura)," *DINAMIKA* 30, no. 1 (2024), hlm. 9507, https://jim.unisma.ac.id/index.php/jdh/article/view/23686/17717.

[9] Giovanno Halbert, Shelvi Rusdiana, and Rufinus Hotmaulana Hutauruk, "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia," *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, no. 3 (December 21, 2023), hlm. 317, https://doi.org/10.55809/tora.v9i3.275.

negara tersebut memiliki kerangka pelindungan data yang kuat dan diakui di kawasan Asia Tenggara. Penelitian ini akan membahas dua poin utama, *pertama*, bagaimana peran dan tanggung jawab LPPDP Indonesia dalam melindungi data pribadi di sektor pemerintahan. *Kedua*, bagaimana perbandingan rancangan LPPDP Indonesia dengan lembaga pelindungan data pribadi di Singapura dalam mencegah pelanggaran data pribadi di sektor pemerintahan. Dengan mempelajari praktik-praktik terbaik dari lembaga tersebut, diharapkan LPPDP Indonesia dapat merumuskan kebijakan yang lebih kuat dan efektif dalam menegakkan hukum terhadap pelanggaran data pribadi.

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif (*normatif legal research*) dengan pendekatan perbandingan (*comparative approach*) dan pendekatan peraturan perundang-undangan (*statute approach*). Pendekatan perbandingan diterapkan untuk menilai perbedaan dan persamaan dalam sistem perlindungan data pribadi antara Indonesia dan Singapura, khususnya dalam hal pembentukan, sistem kerja, dan efektivitas lembaga pengawas pelindungan data pribadi. Adapun pendekatan peraturan perundang-undangan digunakan untuk menelaah ketentuan yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia dan Personal Data Protection Act 2012 (PDPA) di Singapura sebagai dasar hukum utama dalam penelitian ini.

Bahan hukum yang digunakan dalam penelitian ini terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer terdiri dari Undang-Undang Nomor 27 Tahun 2022 yang menjadi sumber utama dalam memahami prinsip dan esensi perlindungan yang diperlukan untuk data pribadi di Indonesia, serta Personal Data Protection Act (PDPA) 2012 di Singapura, yang berperan sebagai perbandingan dalam mengidentifikasi praktik terbaik dalam pelindungan data pribadi. Bahan hukum sekunder mencakup literatur, jurnal hukum, artikel ilmiah, dan penelitian terkait yang memberikan perspektif tambahan dan membantu analisis dalam memahami sistem pelindungan data pribadi di masing-masing negara.

Pengumpulan data dilakukan melalui studi pustaka (*library research*), di mana penulis menelaah dan menganalisis berbagai dokumen hukum serta literatur relevan untuk memperkaya pemahaman tentang hukum pelindungan data pribadi di Indonesia dan Singapura. Teknik analisis data dilakukan secara kualitatif dengan menyusun, mengolah, serta membandingkan bahan hukum primer dan sekunder. Hasil analisis ini akan menggambarkan kesamaan, perbedaan, serta efektivitas penegakan hukum terkait pelindungan data pribadi di kedua negara.

3. PEMBAHASAN

3.1 Peran dan Tanggung Jawab Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) dalam Melindungi Data Pribadi

Kehadiran regulator atau otoritas yang mampu menegakkan aturan dalam UU Pelindungan Data Pribadi (UU PDP) sangat diperlukan untuk memastikan

akuntabilitas dan efektivitas dalam penerapannya. Kedua aspek ini harus menjadi fokus utama agar hak-hak individu atau subjek data terlindungi dengan baik. Hal ini sejalan dengan pandangan Mochtar Kusumaatmadja yang menyatakan bahwa hukum terdiri dari empat unsur utama: kaidah, asas, lembaga, dan proses. Keberadaan lembaga yang bertugas melaksanakan pelindungan data pribadi menjadi tolok ukur penting dalam menilai efektivitas penerapan hukum di masyarakat. Sebagai salah satu pilar hukum, lembaga tersebut berperan penting dalam mewujudkan asas dan kaidah hukum dalam kenyataan sehari-hari.[10]

Kelembagaan pelindungan data pribadi diatur dalam Undang-Undang Pelindungan Data Pribadi (UU PDP), khususnya dalam Bab IX yang mencakup Pasal 58 hingga Pasal 61. UU ini mengamanatkan pembentukan lembaga yang bertanggung jawab atas pelindungan data pribadi, yang disebut sebagai Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP).[11] Menurut Pasal 58 ayat (2), LPPDP adalah lembaga yang dibentuk oleh pemerintah untuk menjalankan fungsi pelindungan data pribadi. Fungsi utama lembaga ini, sebagaimana diatur dalam Pasal 59, mencakup perumusan kebijakan, pengawasan, serta penegakan hukum administratif terkait pelindungan data pribadi. Selain itu, berdasarkan Pasal 58 ayat (4), lembaga ini bertanggung jawab langsung kepada Presiden. Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) memiliki sejumlah tugas dan wewenang yang diatur dalam Pasal 59 dan Pasal 60 UU PDP. Pasal 59 secara rinci memaparkan tugas pokok Lembaga Pelaksana Pelindungan Data Pribadi, meliputi:

1. Perumusan kebijakan: LPPDP bertanggung jawab untuk menyusun dan menetapkan kebijakan serta strategi pelindungan data pribadi yang menjadi pedoman bagi subjek data, pengendali data, dan prosesor data pribadi.
2. Pengawasan: Lembaga ini mengawasi kepatuhan para pengendali data dalam melaksanakan pelindungan data pribadi sesuai dengan ketentuan yang berlaku.
3. Penegakan hukum administratif: LPPDP berwenang menegakkan hukum administratif terkait pelanggaran pelindungan data pribadi, termasuk menjatuhkan sanksi administratif kepada pihak yang melanggar.
4. Fasilitasi penyelesaian sengketa: LPPDP berperan dalam memfasilitasi penyelesaian sengketa yang berkaitan dengan pelanggaran data pribadi melalui mekanisme di luar pengadilan.[12]

Berdasarkan Pasal 60 UU PDP, wewenang LPPDP dapat dikelompokkan menjadi lima kategori utama. Pertama, LPPDP bertugas merumuskan kebijakan di bidang pelindungan data pribadi. Kedua, lembaga ini memiliki wewenang mengawasi kepatuhan terhadap peraturan dan menjatuhkan sanksi atas pelanggaran yang terjadi. Ketiga, LPPDP juga berperan dalam menjalin kerja sama internasional

[10] *Ibid*,. hlm.7.
[11] *Ibid*,. hlm. 7.
[12] Undang-undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

di bidang pelindungan data. Keempat, lembaga ini menerima dan menindaklanjuti aduan serta menyelesaikan sengketa terkait pelanggaran data. Terakhir, LPPDP bertanggung jawab untuk memantau perkembangan teknologi yang relevan dengan pelindungan data pribadi.

1. Perumusan Kebijakan
    a. Pasal 60 huruf a: Merumuskan dan menetapkan kebijakan di bidang pelindungan data pribadi.
2. Pengawasan dan Penegakan Hukum
    a. Pasal 60 huruf b: Melakukan pengawasan terhadap kepatuhan pengendali data pribadi.
    b. Pasal 60 huruf c: Menjatuhkan sanksi administratif atas pelanggaran pelindungan data pribadi yang dilakukan oleh pengendali data dan/atau prosesor data pribadi.
    c. Pasal 60 huruf d: Membantu aparat penegak hukum dalam penanganan dugaan tindak pidana data pribadi.
3. Kerja sama Internasional
    a. Pasal 60 huruf e: Bekerja sama dengan lembaga pelindungan data pribadi negara lain dalam penyelesaian dugaan pelanggaran lintas negara.
4. Penanganan Aduan dan Penyelesaian Sengketa
    a. Pasal 60 huruf f: Melakukan penilaian terhadap pemenuhan persyaratan transfer data pribadi ke luar wilayah Indonesia.
    b. Pasal 60 huruf i: Menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran pelindungan data pribadi.
    c. Pasal 60 huruf j: Melakukan penyelidikan atas pengaduan, laporan, dan/atau hasil pengawasan terhadap dugaan pelanggaran pelindungan data pribadi.
    d. Pasal 60 huruf o: Meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa pelindungan data pribadi.
5. Akses dan Pengawasan Teknologi
    a. Pasal 60 huruf g: Memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada pengendali data pribadi dan/atau prosesor data pribadi.
    b. Pasal 60 huruf h: Melakukan publikasi hasil pelaksanaan pengawasan pelindungan data pribadi sesuai dengan peraturan.
    c. Pasal 60 huruf k: Memanggil dan menghadirkan setiap orang dan/atau badan publik yang terkait dengan dugaan pelanggaran pelindungan data pribadi.
    d. Pasal 60 huruf l: Meminta keterangan, data, informasi, dan dokumen dari setiap orang dan/atau badan publik terkait dugaan pelanggaran pelindungan data pribadi.

e. Pasal 60 huruf m: Memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaan pelanggaran pelindungan data pribadi.
f. Pasal 60 huruf n: Melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan pengendali data pribadi dan/atau prosesor data pribadi.[13]

LPPDP memiliki cakupan wewenang yang sangat luas dalam memastikan pelindungan data pribadi, mulai dari merumuskan kebijakan, mengawasi pelaksanaan, menegakkan hukum, hingga menangani sengketa dan kerja sama internasional. Pasal 60, yang memberikan 15 kewenangan kepada Lembaga Pelindungan Data Pribadi, mencerminkan komitmen Indonesia dalam memenuhi janji untuk melindungi data pribadi sesuai dengan standar internasional. Pengaturan ini sejalan dengan regulasi pelindungan data pribadi di berbagai negara, terutama di kawasan Asia Tenggara, dan mendekati standar minimal yang diterapkan secara global.[14] LPPDP memiliki tanggung jawab dalam penegakan hukum atas pelanggaran terhadap pelindungan data pribadi, termasuk di sektor pemerintahan. Berdasarkan Pasal 57, terdapat dua jenis sanksi yang dapat diterapkan oleh LPPDP: sanksi administratif dan pidana.

1. Sanksi Administratif: Untuk pelanggaran ringan atau kesalahan teknis, LPPDP dapat menjatuhkan sanksi administratif seperti peringatan tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan data pribadi, dan denda administratif. Sanksi denda administratif dapat mencapai 2% dari pendapatan tahunan entitas pelanggar.
2. Sanksi Hukum: Untuk pelanggaran yang lebih berat, LPPDP dapat bekerja sama dengan aparat penegak hukum untuk membawa kasus ke pengadilan. Sesuai dengan Pasal 67, hukuman pidana atas pelanggaran berat, seperti mengakses atau menggunakan data pribadi secara ilegal, dapat mencapai 5 tahun penjara atau denda hingga Rp5 miliar.[15]

Selain mencakup pelindungan data pribadi di dalam negeri, UU PDP juga menerapkan asas ekstrateritorial. Penerapan prinsip yurisdiksi ekstrateritorial bertujuan untuk mencapai tiga aspek penting. Pertama, untuk mengontrol dan memengaruhi perilaku individu. Kedua, untuk mengawasi dan mengatur perilaku korporasi. Ketiga, untuk mempengaruhi kebijakan serta perilaku negara lain.[16] Selaras dengan tujuan tersebut, UU PDP tidak hanya mengatur entitas di dalam

[13] *Ibid*,. hlm. 8.
[14] Gunawan Widjaja and Fransiska Milenia Cesarianti, "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 dan Pasal 60 Undang–Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (April 24, 2024), hlm. 238-239, https://doi.org/10.62335/8qf44b59.
[15] Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
[16] Punra Cita Nugraha, *Yurisdiksi Dalam Hukum Siber* (Bandung: REFIKA, 2022), hlm. 67.

negeri, tetapi juga memberikan kewenangan untuk memantau perilaku individu maupun perusahaan yang beroperasi di luar negeri, selama tindakan mereka berdampak pada data pribadi warga Indonesia. Hal ini secara eksplisit disebutkan dalam pasal 2 UU PDP yang menyebutkan bahwa undang-undang ini berlaku tidak hanya untuk orang, badan publik, dan organisasi internasional yang berada di wilayah hukum Indonesia, tetapi juga bagi pihak-pihak di luar wilayah Indonesia yang memiliki akibat hukum:

1. Di wilayah hukum Negara Republik Indonesia, dan/atau
2. Bagi subjek data pribadi warga negara Indonesia di luar wilayah hukum Indonesia.[17]

Dengan demikian, penerapan yurisdiksi ekstrateritorial ini bertujuan untuk memastikan bahwa pelindungan terhadap data pribadi warga Indonesia tetap terjamin, baik di dalam maupun di luar negeri, sesuai dengan standar yang diatur dalam UU PDP.

3.2 Tinjauan Lembaga Pelindungan Data Pribadi di Singapura sebagai Perbandingan Rancangan LPPDP Indonesia

Pelindungan data pribadi di Singapura memiliki dua lembaga utama yang bertanggung jawab atas pengelolaan dan penegakan hukum pelindungan data, yaitu Personal Data Protection Commission (PDPC) di sektor swasta dan Smart Nation and Digital Government Group (SNDGG) di sektor publik. Kedua lembaga ini memiliki peran dan tanggung jawab yang berbeda namun saling melengkapi dalam memastikan keamanan dan privasi data pribadi di Singapura.

3.2.1 Personal Data Protection Commission (PDPC)

Personal Data Protection Commission (PDPC) Singapura merupakan lembaga independen yang bertanggungjawab atas pelindungan data pribadi di negara tersebut. Didirikan berdasarkan Undang-Undang Pelindungan Data Pribadi (PDPA), PDPC memiliki mandat untuk memastikan bahwa organisasi yang mengelola data pribadi individu mematuhi hukum dan prinsip-prinsip pelindungan data yang berlaku. PDPC berperan sebagai regulator, pengawas, dan edukator. Sebagai regulator, PDPC mengeluarkan pedoman dan peraturan terkait pelindungan data. Sebagai pengawas, PDPC melakukan investigasi terhadap pelanggaran PDPA dan dapat menjatuhkan sanksi. Dan sebagai edukator, PDPC memberikan bimbingan dan pelatihan kepada organisasi dan individu mengenai cara mengelola data pribadi secara aman dan bertanggungjawab.[18]

3.2.2 Struktur dan Kewenangan Lembaga Personal Data Protection Commission (PDPC)

[17] Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi..

[18] Personal Data Protection Commission, "About Us," accessed September 10, 2024, https://www.pdpc.gov.sg/who-we-are/about-us.

Personal Data Protection Commission (PDPC) adalah lembaga yang bertugas mengelola Undang-Undang Pelindungan Data Pribadi (Personal Data Protection Act - PDPA) di Singapura. Menurut Pasal 5(1), PDPC berada di bawah naungan Info-communications Media Development Authority (IMDA), sebuah badan otonom yang berada di bawah Kementerian Komunikasi dan Informasi Singapura. IMDA bertanggung jawab untuk mengembangkan sektor informasi, komunikasi, serta media di negara tersebut. Berdasarkan Pasal 5(2), PDPC bertanggung jawab atas administrasi serta penerapan PDPA. Selain itu, PDPC memiliki tugas pengawasan dan penegakan aturan yang diatur dalam Pasal 10(1), yang memungkinkan PDPC bekerja sama dengan badan regulator lain jika diperlukan.[19]

Fungsi utama PDPC, sebagaimana diatur dalam Pasal 6, adalah sebagai berikut:

1. Promosi Kesadaran Pelindungan Data: Meningkatkan kesadaran masyarakat tentang pentingnya pelindungan data di Singapura.
2. Layanan Konsultasi: Menyediakan konsultasi serta layanan ahli yang berkaitan dengan pelindungan data.
3. Nasihat kepada Pemerintah: Memberikan nasihat kepada pemerintah terkait isu-isu pelindungan data.
4. Penegakan Hukum: Menegakkan peraturan dan mengelola pelaksanaan undang-undang pelindungan data di Singapura.[20]

3.2.3 Proses Penanganan Pelanggaran Data Pribadi

Ketika terjadi pelanggaran data pribadi, proses penanganan kasus akan melibatkan beberapa tahapan penting. Mulai dari pengajuan keluhan oleh individu yang merasa dirugikan, dilanjutkan dengan investigasi mendalam oleh PDPC, hingga pemberian sanksi bagi pihak yang terbukti melanggar. Setiap tahapan dalam proses ini memiliki tujuan yang jelas, yaitu untuk memastikan bahwa hak-hak individu terlindungi dan pelaku pelanggaran bertanggung jawab atas perbuatannya. Mekanisme terkait Penanganan pelanggaran juga telah diatur dalam pasal-pasal PDPA.

1. Pengajuan Keluhan

   Setiap individu yang merasa bahwa hak privasinya telah dilanggar oleh organisasi dapat mengajukan keluhan kepada PDPC. Hal ini tertuang dalam pasal 48H yaitu, PDPC memiliki kewenangan untuk meninjau dan menilai keluhan tersebut.
2. Investigasi

   PDPC diberi kewenangan untuk melakukan penyelidikan terhadap dugaan pelanggaran pelindungan data oleh organisasi. Hal ini tertuang

[19] Government of Singapore, "Personal Data Protection Act 2012" (Singapore Statutes Online), accessed September 7, 2024, https://sso.agc.gov.sg/Act/PDPA2012.

[20] *Ibid*,.

dalam pasal 50 yaitu, PDPC dapat meminta bukti, memanggil saksi, dan melakukan tindakan investigasi lainnya.

3. Pemberian Sanksi

   Jika ditemukan pelanggaran, maka PDPC dapat memberikan arahan kepada organisasi untuk mematuhi PDPA atau memberikan sanksi berupa denda. Hal ini tertuang dalam pasal 48J yaitu, PDPC dapat mengeluarkan denda hingga jumlah tertentu yang ditentukan jika organisasi tidak mematuhi undang-undang.

4. Transparansi kepada Publik

   PDPC dapat mengumumkan hasil investigasi dan sanksi kepada publik sebagai bentuk transparansi dan untuk mengedukasi masyarakat. Hal ini tertuang dalam pasal 49 yaitu, PDPC juga dapat menerbitkan panduan atau rekomendasi terkait pelanggaran untuk membantu organisasi mematuhi PDPA.[21]

3.2.4 Sanksi dan Kewajiban terhadap Lembaga Pemerintahan

Sanksi yang dikenakan kepada lembaga pemerintah tidak diatur secara langsung oleh Undang-Undang Pelindungan Data Pribadi (Personal Data Protection Act - PDPA). Namun, pelindungan data dalam lembaga pemerintah tetap diatur melalui peraturan internal yang mengacu pada prinsip-prinsip pelindungan data yang kuat. Data pribadi yang dikelola oleh lembaga pemerintah tidak terlepas dari pelindungan yang ketat. Hal ini ditegaskan dalam Pasal 4(1)(c) yang menyatakan bahwa kewajiban yang tercantum dalam Bagian III hingga VI dari PDPA tidak berlaku untuk lembaga pemerintah.[22] Dengan demikian, lembaga pemerintah dikecualikan dari beberapa ketentuan penting PDPA dan tidak dikenakan sanksi yang sama dengan sektor swasta.

Meskipun lembaga pemerintah tidak terikat oleh kewajiban yang sama seperti sektor swasta, mereka tetap memiliki tanggung jawab dalam melindungi data pribadi. Berikut adalah beberapa kewajiban utama terkait regulasi pelindungan data di sektor pemerintahan:

1. Pasal 4(1)(c): Bagian III hingga VI dari PDPA tidak berlaku untuk lembaga pemerintah, sehingga mereka tidak terikat oleh kewajiban yang sama seperti organisasi di sektor swasta.
2. Data *Intermediary* Pemerintah: Lembaga pemerintah dapat menunjuk pihak ketiga atau data *intermediary* untuk memproses data pribadi atas nama mereka. Meskipun lembaga pemerintah dikecualikan dari beberapa ketentuan PDPA, data intermediary yang ditunjuk tetap harus mematuhi aturan PDPA dalam konteks pengolahan data untuk lembaga pemerintah. Hal ini diatur dalam Pasal 26E.[23]

[21] *Ibid*,.
[22] *Ibid*,.
[23] *Ibid*,.

Secara keseluruhan, meskipun lembaga pemerintah memiliki pengecualian dari beberapa ketentuan PDPA, regulasi internal serta pengawasan ketat tetap diberlakukan untuk memastikan bahwa data pribadi yang mereka kelola tetap dilindungi dengan baik

3.3 Smart Nation and Digital Government Group (SNDGG)

Personal Data Protection Commission (PDPC) tidak mengatur secara langsung pelindungan terkait data pribadi di lembaga pemerintahan. Namun, pengelolaan data pribadi di sektor publik diatur oleh Smart Nation and Digital Government Group (SNDGG) dan telah dijamin melalui Public Sector Governance Act 2018.[24] SNDGG merupakan sebuah kelompok kerja di bawah *Prime Minister's Office* atau Kantor Perdana Menteri Singapura yang memiliki tugas utama untuk memimpin transformasi digital di negara tersebut. Mereka bertanggung jawab dalam merancang, mengembangkan, dan mengimplementasikan berbagai inisiatif teknologi untuk meningkatkan kualitas hidup masyarakat dan efisiensi pemerintahan.[25] SNDGG juga bekerja sama dengan Government Technology Agency (*GovTech*) untuk memastikan keamanan serta privasi data di lingkungan pemerintahan. SNDGG dibentuk melalui keputusan pemerintah sebagai bagian dari inisiatif *Smart Nation* yang dikoordinasikan oleh kantor Perdana Menteri Singapura pada tahun 2017. Struktur dan kewenangannya didasarkan pada kebijakan dan arahan eksekutif pemerintah, bukan pada undang-undang formal tertentu.[26]

3.3.1 Struktur dan Fungsi Smart Nation and Digital Government Group (SNDGG)

Struktur organisasi Smart Nation and Digital Government Group (SNDGG) di Singapura dirancang untuk memimpin dan mengoordinasikan upaya transformasi digital di seluruh pemerintahan melalui dua unit utama yaitu Smart Nation and Digital Government Office (SNDGO) dan Government Technology Agency (GovTech).

Unit pertama, SNDGO, bertanggung jawab atas perumusan kebijakan dan pengembangan strategi digital nasional. SNDGO memimpin inisiatif besar terkait Smart Nation, memastikan koordinasi lintas kementerian dan lembaga pemerintah dalam pelaksanaan kebijakan digital. Tim SNDGO terdiri dari anggota berbagai unit sebelumnya, termasuk Smart Nation Programme Office (SNPO), Direktorat *Digital Government* dari Kementerian Keuangan (MOF), serta Departemen Kebijakan Teknologi Pemerintah di Kementerian

[24] Tiara Almira Raila, Sinta Dewi Rosadi, and Rika Ratna Permata, "Perlindungan Data Privasi di Indonesia dan Singapura Terkait Penerapan Digital Contact Tracing sebagai Upaya Pencegahan Covid-19 serta Tanggungjawabnya," *Jurnal Kepastian Hukum dan Keadilan* 2, no. 1 (January 13, 2021), hlm. 2.

[25] Smart Nation and Digital Government Office, "Ministerial Committee," accessed September 10, 2024, https://www.smartnation.gov.sg/archive/ministerial-committee/.

[26] "Singapore's Smart Nation Initiative – A Policy and Organisational Perspective," *The Lee Kuan Yew School of Public Policy at the National University of Singapore*, accessed September 10, 2024, https://lkyspp.nus.edu.sg/docs/default-source/case-studies/singapores-smart-nation-initiative-final_112018.pdf?sfvrsn=354e720a_2, hlm. 8-9.

Komunikasi dan Informasi (MCI). Tugas utama SNDGO adalah menyelaraskan visi digital nasional dan mengarahkan kebijakan yang mendukung transformasi digital di sektor pemerintahan.

Unit kedua, GovTech, bertugas mengimplementasikan kebijakan yang dirumuskan oleh SNDGO. GovTech memainkan peran penting dalam mengembangkan dan menerapkan solusi teknologi untuk mendukung digitalisasi layanan publik, seperti sistem identitas digital, pembayaran elektronik, dan pengelolaan infrastruktur data. Struktur organisasi ini dirancang untuk mendorong kolaborasi lintas sektor dan lembaga, memastikan kebijakan digital berjalan selaras, dan mendukung transformasi digital yang efisien di seluruh Singapura.

SNDGG memiliki beberapa kewenangan utama untuk mendorong transformasi digital di Singapura. Berikut adalah kewenangan utama mereka:

1. Koordinasi Digital Lintas Kementerian: SNDGG berfungsi sebagai pusat pengkoordinasi untuk upaya digitalisasi di seluruh kementerian dan lembaga pemerintah, memastikan kebijakan digital yang selaras dan terintegrasi.
2. Pengembangan Kebijakan Smart Nation: Melalui Smart Nation and Digital Government Office (SNDGO), SNDGG merumuskan kebijakan untuk inisiatif *Smart Nation*, mencakup sektor seperti transportasi pintar, pelayanan kesehatan digital, dan layanan pemerintah berbasis digital.
3. Pelaksanaan Teknologi Digital: SNDGG, melalui Government Technology Agency (GovTech), mengawasi pengembangan dan implementasi solusi teknologi untuk layanan publik, seperti identitas digital dan pembayaran elektronik.
4. Mendorong Inovasi dan Penelitian: SNDGG mendukung inovasi dengan investasi dalam penelitian dan pengembangan (R&D), serta berkolaborasi dengan sektor swasta dan masyarakat melalui program *seperti Smart Nation Fellowship Programme*.
5. Membangun Infrastruktur Digital Nasional: SNDGG bertanggung jawab memastikan adanya infrastruktur digital yang kuat, termasuk jaringan *broadband* nasional, platform data terbuka, dan sistem keamanan siber.
6. Meningkatkan Efisiensi Layanan Publik: SNDGG berfokus pada peningkatan efisiensi dan aksesibilitas layanan publik melalui digitalisasi, termasuk layanan *online* yang lebih baik dan integrasi data antar lembaga.[27]

[27] *Ibid*,.hlm. 8-9.

3.4 Perbandingan dan Penerapan Praktik Pelindungan Data Pribadi di Singapura sebagai Acuan LPPDP di Indonesia

Analisis komparatif rancangan LPPDP Indonesia dengan lembaga pelindungan data di Singapura berfokus pada upaya penegakan hukum terkait pelanggaran data pribadi di sektor pemerintahan. Berikut ini adalah tabel yang dapat memperjelas perbedaan utama dari SNDGG, PDPC, dan LPPDP sehingga memberikan pemahaman yang lebih jelas mengenai peran masing-masing lembaga dalam pengelolaan transformasi digital serta pelindungan data pribadi.

TABEL 1
Perbandingan SNDGG dan PDPC dengan LPPDP Indonesia[28]

Aspek	PDPC (Singapura)	SNDGG (Singapura)	LPPDP (Indonesia)
Status Lembaga	Independen, di bawah IMDA	Di bawah Kantor Perdana Menteri	Di bawah pengawasan pemerintah
Landasan Hukum	Personal Data Protection Act (PDPA)	Kebijakan pemerintah, bukan undang-undang formal	Undang-Undang Pelindungan Data Pribadi (UU PDP)
Fokus Utama	Pelindungan data pribadi di sektor swasta	Pengelolaan transformasi digital dan keamanan data di sektor publik	Pelindungan data pribadi di sektor publik dan swasta
Otoritas Penegakan Hukum	Investigasi, pemberian sanksi denda, arahan perbaikan	Tidak memiliki kewenangan penegakan hukum, fokus pada infrastruktur digital	Penegakan hukum administratif, sanksi pidana dan denda
Transparansi	Hasil investigasi dan sanksi diumumkan ke publik	Tidak memiliki mekanisme transparansi publik	Publikasi hasil pelaksanaan pengawasan sesuai dengan peraturan yang berlaku
Peran Edukasi	Memberikan bimbingan dan pelatihan kepada organisasi dan individu	Fokus pada pengembangan infrastruktur digital, bukan edukasi publik	Tidak mengedukasi masyarakat secara langsung, tetapi memfasilitasi peran publik dalam mendukung pelindungan data pribadi.
Kolaborasi Internasional	Aktif dalam kerja sama internasional	Tidak terlibat dalam kerja sama internasional	Memungkinkan kerja sama internasional,
Sektor Publik	Tidak mengawasi sektor publik (tanggung jawab SNDGG)	Bertanggung jawab atas transformasi digital dan keamanan data	Diawasi oleh LPPDP

[28] Diolah oleh Penulis berdasarkan UU No. 27 Tahun 2022, PDPA 2012, dan literatur terkait

PDPC di Singapura berada di bawah IMDA (Info-communications Media Development Authority), tetapi tetap memiliki status independen dalam mengawasi pelaksanaan Personal Data Protection Act (PDPA) di sektor swasta. Namun, kelembagaan PDPC masih bisa dipengaruhi oleh pemerintah melalui penunjukan dan pemberhentian pimpinan yang bisa dilakukan kapan saja oleh Kementerian Komunikasi dan Informasi Singapura (MCI). Adapun SNDGG, yang bertanggung jawab atas keamanan data di sektor publik, berada di bawah Kantor Perdana Menteri dan berfungsi untuk mengelola transformasi digital pemerintah. Meskipun bukan lembaga pengawas, SNDGG menjaga keamanan data yang dikelola oleh pemerintah.[29] LPPDP di Indonesia sebaiknya didesain sebagai lembaga yang benar-benar independen untuk menghindari campur tangan politik atau pemerintah. Penempatan di bawah kementerian, seperti Kemenkominfo, bisa mengurangi independensi dan mempengaruhi objektivitas dalam penegakan hukum. Model independensi seperti PDPC lebih cocok diterapkan, dengan tetap memberi ruang kontrol terhadap lembaga tersebut melalui mekanisme yang melibatkan DPR, sehingga tidak ada pengaruh politik tunggal.[30]

PDPC berfokus pada pengawasan sektor swasta, memastikan organisasi mematuhi aturan pelindungan data. PDPC memiliki kewenangan penuh untuk melakukan investigasi, menjatuhkan sanksi denda, dan memberikan arahan kepada organisasi yang melanggar. Adapun SNDGG menangani sektor publik, memastikan keamanan data dan transformasi digital instansi pemerintah melalui kerja sama dengan GovTech. LPPDP dapat mengadopsi pendekatan ini untuk sektor publik, bekerja sama dengan lembaga lain seperti BSSN dan Kementerian Komunikasi dan Informatika (Kemenkominfo) dalam menjaga keamanan data di sistem elektronik pemerintahan, terutama di tengah upaya Indonesia menuju *smart city* di Ibu Kota Negara (IKN) Nusantara.

PDPC di Singapura memiliki mekanisme penegakan hukum yang efektif, dengan sanksi tegas terhadap pelanggaran data, termasuk denda hingga SGD 1 juta (sekitar Rp11 miliar). Mekanisme ini juga transparan, dengan hasil investigasi dan sanksi diumumkan kepada publik untuk meningkatkan kepatuhan dan menjaga kepercayaan. Adapun SNDGG tidak memiliki kewenangan untuk memberikan sanksi, tetapi bertanggung jawab menjaga keamanan data melalui infrastruktur teknologi yang kuat di sektor pemerintahan. LPPDP harus memiliki mekanisme penegakan hukum yang transparan dan tegas. Sanksi administrasi dan pidana harus dapat dijalankan secara efektif, dengan pengumuman publik terhadap pelanggaran untuk meningkatkan kesadaran dan kepatuhan.

[29] Azza Fitrahul Faizah et al., "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," *Hakim: Jurnal Ilmu Hukum dan Sosial* 1, no. 3 (2023), hlm. 17, https://doi.org/10.51903/hakim.v1i3.1222.

[30] *Ibid*,. hlm. 20.

PDPC tidak hanya berfungsi sebagai pengawas, tetapi juga sebagai edukator yang memberikan pelatihan kepada organisasi dan publik tentang pentingnya pelindungan data pribadi dan bagaimana mengelolanya dengan benar. LPPDP dapat mengadopsi peran serupa, memberikan pelatihan, bimbingan, dan sosialisasi terkait pelindungan data kepada publik dan organisasi. Edukasi ini penting untuk membangun kesadaran masyarakat akan hak-hak mereka terkait data pribadi serta membantu organisasi memahami tanggung jawab mereka dalam melindungi data.

Contoh implementasi di Indonesia misalnya insiden kebocoran data yang pernah terjadi, sebanyak 337 juta data pribadi yang disimpan oleh Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil), Kementerian Dalam Negeri (Kemendagri), diduga bocor dan dijual di forum peretas BreachForums. Data yang bocor mencakup Nama, Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), alamat, tanggal lahir, dan informasi sensitif lainnya. Selain itu, pemerintah juga mengakui serangan *ransomware* oleh kelompok Lockbit 3.0 pada Pusat Data Nasional Sementara (PDNS) 2 yang terjadi pada 20 Juni 2024, menyebabkan gangguan besar pada infrastruktur data pemerintah.[31]

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kemenkominfo) dan Badan Siber dan Sandi Negara (BSSN) kemudian ditugaskan untuk melakukan penyelidikan terhadap kebocoran data di Dukcapil. Namun, hasil penyelidikan seringkali tidak transparan, dan publik tidak mendapatkan informasi yang jelas mengenai langkah-langkah yang diambil oleh pemerintah. Teguh Aprianto, pendiri Ethical Hacker Indonesia, sebuah komunitas peretasan etis yang bertujuan untuk melawan kejahatan siber, mengkritik respons pemerintah yang dianggap terburu-buru membantah kebocoran data sebelum investigasi yang mendalam dilakukan.[32]

Kasus-kasus ini menunjukkan adanya kekurangan sistemik dalam tata kelola dan pelindungan data pribadi di sektor pemerintah Indonesia. Belum adanya lembaga khusus yang bertanggung jawab penuh atas pelindungan data pribadi membuat mekanisme penegakan hukum dan pelindungan terhadap data pribadi menjadi lemah. Pemerintah melalui Kemenkominfo dan BSSN bertanggung jawab untuk menangani insiden Kasus kebocoran data Dukcapil dan serangan PDNS. Namun, beberapa tantangan utama yang dihadapi adalah:

1. Hasil investigasi sering tidak diumumkan kepada publik, sehingga masyarakat tidak tahu langkah apa yang telah diambil untuk mencegah kebocoran data di masa depan.

[31] Tim CNN Indonesia, "Fakta-Fakta Kebocoran Data PDNS, Dalang Hingga Jumlah Tebusan," *CNN Indonesia*, June 25, 2024, https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan.

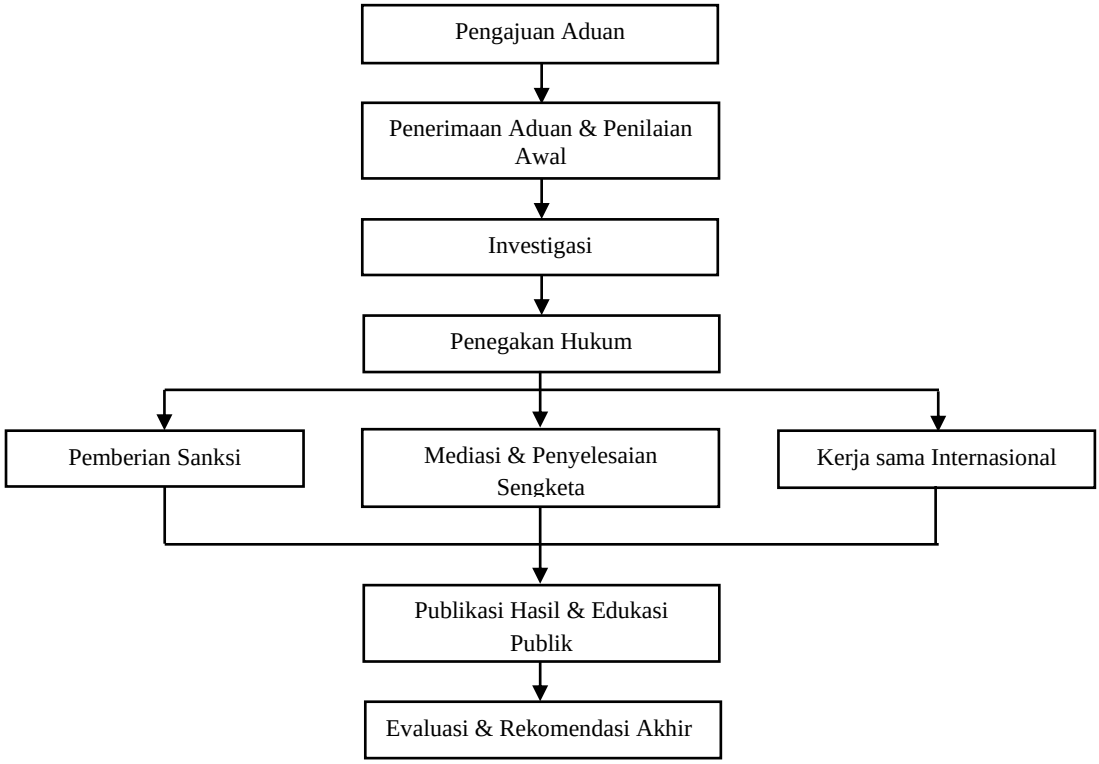
[32] Fea, "337 Juta Data Dukcapil Diduga Bocor Dan Dijual Di Forum Hacker," *CNN Indonesia*, July 16, 2023, https://www.cnnindonesia.com/teknologi/20230716223757-192-974143/337-juta-data-dukcapil-diduga-bocor-dan-dijual-di-forum-hacker.

2. Pemerintah hanya bisa memberikan sanksi teguran, tanpa adanya lembaga khusus yang secara penuh memiliki wewenang untuk menindak pelanggaran data pribadi.
3. Keterbatasan dalam menangani pelanggaran lintas negara seperti dalam kasus Lockbit 3.0, yang merupakan kelompok peretas internasional, pemerintah Indonesia kesulitan menjatuhkan sanksi karena belum meratifikasi Konvensi Cybercrime.[33]

Pembentukan Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) yang independen, mengadopsi model Singapura, akan memberikan kewenangan penuh dalam mengawasi dan menangani pelanggaran data pribadi di Indonesia. Dalam kasus kebocoran data seperti yang terjadi pada Dukcapil dan PDNS, LPPDP akan bertindak dengan cepat melalui langkah-langkah yang terstruktur. Pertama, LPPDP segera melakukan investigasi independen terhadap kebocoran data, mengumpulkan bukti, dan memanggil pihak-pihak yang terlibat. Proses ini akan dilakukan secara profesional dan terbuka kepada publik, meningkatkan transparansi. Kedua, jika terbukti adanya pelanggaran terhadap regulasi pelindungan data pribadi (UU PDP), LPPDP akan menjatuhkan sanksi denda yang tegas, sesuai dengan ketentuan UU PDP. Misalnya, denda administratif bisa mencapai 2% dari pendapatan tahunan entitas pelanggar, yang dapat memberikan efek jera. Kemudian hasil dari investigasi akan diumumkan kepada publik untuk memberikan kejelasan tentang tindakan yang diambil dan untuk mengembalikan kepercayaan masyarakat terhadap sistem pelindungan data. Berikut adalah diagram alur proses penyelesaian pelanggaran data pribadi yang diusulkan untuk LPPDP, dimulai dari pengajuan aduan hingga publikasi hasil dan rekomendasi perbaikan.

BAGAN I
Alur Penyelesaian Pelanggaran Data Pribadi oleh LPPDP[34]

[33] Tim CNN Indonesia, “Fakta-Fakta Kebocoran Data PDNS, Dalang Hingga Jumlah Tebusan.”
[34] Diolah oleh Penulis



Alur penyelesaian ini dirancang untuk memastikan bahwa setiap kasus pelanggaran data pribadi dapat ditangani secara sistematis dan adil. Proses mediasi memberikan kesempatan penyelesaian sengketa yang lebih cepat, sementara penegakan hukum dan pemberian sanksi memastikan adanya konsekuensi yang tegas bagi pelanggaran serius. Misalnya dalam kasus serangan *rensomware* seperti yang terjadi di PDNS oleh kelompok Lockbit 3.0, LPPDP akan bekerja sama dengan lembaga seperti BSSN untuk melakukan pengawasan keamanan data secara berkelanjutan. Tindakan yang akan diambil mencakup audit keamanan rutin serta penanganan dan pemulihan pasca serangan. Jadi LPPDP akan memberlakukan audit rutin pada sistem-sistem elektronik pemerintah, termasuk Pusat Data Nasional, untuk memastikan keamanan data pribadi yang tersimpan. Lembaga ini juga dapat memberikan arahan perbaikan yang wajib dipatuhi oleh instansi terkait. Kemudian LPPDP bersama BSSN akan mengkoordinasikan pemulihan pasca serangan siber, termasuk memulihkan data yang terkena *ransomware* dan memastikan sistem kembali aman sebelum digunakan kembali.

Ketika serangan berasal dari luar negeri seperti dalam kasus Lockbit 3.0, LPPDP akan berkoordinasi dengan lembaga internasional dan negara lain dalam menangani peretas lintas negara. Kerja sama internasional akan mempermudah melakukan penegakan hukum lintas batas. Selain itu, Indonesia juga akan memiliki kesempatan untuk memperkuat kerja sama internasional dalam menghadapi kejahatan siber dengan meratifikasi konvensi *Cybercrime*. Hal ini juga akan membuat asas

ekstrateritorial yang terdapat dalam Pasal 2 UU PDP dapat diberlakukan dengan efektif. Jika LPPDP di Indonesia sudah terbentuk berdasarkan model yang diterapkan di Singapura, kasus-kasus kebocoran data seperti di Dukcapil dan serangan siber di PDNS akan ditangani dengan lebih baik, mulai dari investigasi yang transparan, penegakan hukum yang kuat, hingga pencegahan berkelanjutan. Hal ini akan meningkatkan kepercayaan publik terhadap pelindungan data pribadi di Indonesia.

4. PENUTUP

Kesimpulan yang dapat dihasilkan dalam tulisan ini yakni, pertama, peran dan tanggung jawab Lembaga Pelaksana Pelindungan Data Pribadi (LPPDP) di Indonesia dalam melindungi data pribadi di sektor pemerintahan sangat penting. LPPDP diharapkan menjadi lembaga independen yang bertanggung jawab untuk merumuskan kebijakan, mengawasi kepatuhan, menegakkan hukum, serta menyelesaikan sengketa terkait pelanggaran data pribadi. Dengan adanya LPPDP, sektor pemerintahan dapat terjamin dari kebocoran data yang semakin meningkat, terutama di era digitalisasi dan pembangunan *smart city* di Ibu Kota Nusantara. Lembaga ini juga harus memiliki otoritas untuk memberikan sanksi tegas dan transparan kepada pihak yang melanggar.

Kedua, perbandingan antara LPPDP Indonesia dan Personal Data Protection Commission (PDPC) serta Smart Nation and Digital Government Group (SNDGG) di Singapura menunjukkan adanya kesenjangan dalam hal independensi, struktur, dan kewenangan penegakan hukum. Singapura memiliki sistem pelindungan data pribadi yang lebih mapan, dengan PDPC yang berfokus pada sektor swasta dan SNDGG yang menangani sektor publik. Indonesia perlu mengadopsi mekanisme serupa, di mana LPPDP bersifat independent dan harus mengawasi kedua sektor tersebut, menerapkan sanksi yang tegas, dan bekerja sama dengan lembaga internasional dalam penanganan kasus lintas negara. Hal ini akan memastikan Indonesia memiliki sistem pelindungan data pribadi yang kuat dan berstandar internasional.

DAFTAR PUSTAKA

Jurnal:

Faizah, Azza Fitrahul, Sinta Dewi Rosadi, Garry Gumelar Pratama, and Ananda Fersa Dharmawan. “Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura.” *Hakim: Jurnal Ilmu Hukum dan Sosial* 1, no. 3 (2023): 01–27. https://doi.org/10.51903/hakim.v1i3.1222.

Halbert, Giovanno, Shelvi Rusdiana, and Rufinus Hotmaulana Hutauruk. “Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia.” *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, no. 3 (December 21, 2023): 304–21. https://doi.org/10.55809/tora.v9i3.275.

Raila, Tiara Almira, Sinta Dewi Rosadi, and Rika Ratna Permata. “Perlindungan Data Privasi di Indonesia dan Singapura Terkait Penerapan Digital Contact Tracing sebagai Upaya Pencegahan Covid-19 serta Tanggungjawabnya.” *Jurnal*

Kepastian Hukum dan Keadilan 2, no. 1 (January 13, 2021): 1–16. https://doi.org/10.32502/khdk.v2i1.3044.

Widjaja, Gunawan, and Fransiska Milenia Cesarianti. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 dan Pasal 60 Undang–Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (April 24, 2024): 234–242. https://doi.org/10.62335/8qf44b59.

Buku:

Imail, Asih Widiarti, Dani Muhadiansyah, and Evan Koesumah. *Keamanan Data Pribadi Terkait Penyelenggaraan Pemilu*. Jakarta: TEMPO Publishing, 2024.

Nugraha, Punra Cita. *Yurisdiksi Dalam Hukum Siber*. Bandung: REFIKA, 2022.

Peraturan Perundang-Undangan:

Undang-Undang Dasar Republik Indonesia Tahun 1945 Pasal 28G Ayat 1.

Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Berita:

Arthaputri, Sylvia Faradina Amandasari, Ahmad Syaifudin, and M Fahrudin. "Perlindungan Data Pribadi sebagai Bentuk Perwujudan Cyber Security (Studi Komparatif Indonesia dan Singapura)." *DINAMIKA* 30, no. 1 (2024): 9495–9509. https://jim.unisma.ac.id/index.php/jdh/article/view/23686/17717.

Fea. "337 Juta Data Dukcapil Diduga Bocor Dan Dijual Di Forum Hacker." *CNN Indonesia*, July 16, 2023. https://www.cnnindonesia.com/teknologi/20230716223757-192-974143/337-juta-data-dukcapil-diduga-bocor-dan-dijual-di-forum-hacker.

Woo, Jun Jie. "Singapore's Smart Nation Initiative: A Policy and Organisational Perspective." Lee Kuan Yew School of Public Policy, National University of Singapore, 2018. https://lkyspp.nus.edu.sg/docs/default-source/case-studies/singapores-smart-nation-initiative final_112018.pdf?sfvrsn=354e720a_2.

Media Online:

Government of Singapore, "Personal Data Protection Act 2012" (Singapore Statutes Online), accessed September 7, 2024, https://sso.agc.gov.sg/Act/PDPA2012.

Kominfo. "Keamanan Siber Jadi Kunci Membangun Kota Cerdas IKN." *Kominfo.Go.Id*, November 3, 2023. https://www.kominfo.go.id/content/detail/52710/keamanan-siber-jadi-kunci-membangun-kota-cerdas-ikn/0/berita.

Personal Data Protection Commission. "About Us." Accessed September 10, 2024. https://www.pdpc.gov.sg/who-we-are/about-us.

Smart Nation and Digital Government Office. "Ministerial Committee." Accessed September 10, 2024. https://www.smartnation.gov.sg/archive/ministerial-committee/.

Tim CNN Indonesia. "Fakta-Fakta Kebocoran Data PDNS, Dalang Hingga Jumlah Tebusan." *CNN Indonesia*, June 25, 2024. https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan.