Jurnal Pembangunan Hukum Indonesia
Volume 6, Nomor 3, Tahun 2024, halaman 431-455
Program Magister Hukum, Fakultas Hukum
Universitas Diponegoro

Research Article

Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara

Fanisa Mayda Ayiliani[1*] , Elfia Farida[2]
[1]Program Magister Hukum, Fakultas Hukum, Universitas Diponegoro
[2]Fakultas Hukum, Universitas Diponegoro
[*]fanisamayda18@gmail.com

ABSTRACT

The establishment of a Personal Data Protection Supervisory Authority is urgently needed in implementing Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), as its critical role includes overseeing compliance and facilitating the submission of complaints regarding alleged violations of the PDP Law both domestically and internationally.This study aims to assess the urgency of establishing a Personal Data Protection Supervisory Authority in Indonesia as a measure to protect cross-border personal data transfers and to recommend its formation based on the concept of Independent Regulatory Agencies (IRAs). The research adopts a normative approach, utilizing statutory, conceptual, and comparative methods. Secondary data was collected through literature studies and analyzed qualitatively.The findings reveal that, as of 2024, internet users in Indonesia accounted for 79.50% of the population, amounting to 221,563,479 individuals out of a total population of 278,696,200. At least every internet user has one platform that collects personal data. Cases of personal data breaches frequently occur in Indonesia due to inadequate protection measures. Therefore, Indonesia urgently needs to establish an independent Personal Data Protection Supervisory Authority, adhering to the ideal concept of an independent state institution or Independent Regulatory Agencies (IRAs). This initiative aims to minimize the interference of other authorities in supervision and law enforcement related to personal data protection, especially as cross-border data transfers continue to increase annually.

Keywords: Personal Data Protection*; *Personal Data Monitoring Agency*; *Cross-Border Transfer of Personal Data.

ABSTRAK

Pembentukan Lembaga Pengawas Data Pribadi sangat dibutuhkan dalam penerapan Undang–Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) karena peran krusial yang dipegang adalah fungsi pengawasan dan memfasilitasi penyampaian pengaduan terkait dugaan pelanggaran UU PDP baik dalam negeri maupun luar negeri. Penelitian bertujuan mengkaji urgensi pembentukan Lembaga Pengawas Data Pribadi di Indonesia sebagai upaya pelindungan transfer data pribadi lintas negara dan merekomendasikan pembentukan Lembaga Pengawas Data Pribadi berdasarkan konsep *Independent Regulatory Agencies* (IRAs). Jenis penelitiannya penelitian normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Data sekunder yang digunakan diperoleh menggunakan metode studi kepustakaan, yang dianalisis dengan menggunakan metode kualitatif. Hasil Penelitian menunjukkan bahwa Tahun 2024 pengguna internet di Indonesia mencapai 79.50% dengan kalkulasi 221.563.479 jiwa dari total populasi 278.696.200 penduduk. Setidaknya setiap pengguna Internet memiliki satu *platform* media yang mengumpulkan data pribadi. Kasus kebocoran data pribadi sering kali terjadi di Indonesia dikarenakan pelindungannya yang kurang kuat. Maka dari itu Indonesia perlu segera membentuk lembaga khusus pengawas data pribadi yang

independen berdasarkan konsep ideal lembaga negara independen atau *Independent Regulatory Agencies* (IRAs), dimaksudkan untuk meminimalisasi intervensi kewenangan lembaga lain dalam melakukan pengawasan dan penegakan hukum terkait pelindungan data pribadi mengingat transfer data pribadi lintas negara kian meningkat setiap tahunnya.

Kata Kunci: Lembaga Pengawas Data Pribadi; Pelindungan Data Pribadi; Transfer Data Pribadi Lintas Negara.

A. PENDAHULUAN

Pertukaran data pribadi secara lintas negara kian berkembang dan telah menjadi hal yang umum sekarang ini. Tantangan yang muncul terkait hal ini adalah bagaimana cara melindungi data pribadi individu dari kemungkinan penyalahgunaan oleh berbagai pihak, termasuk pemerintah dan perusahaan swasta. Informasi beredar secara global melalui jaringan yang tidak terbatas. Meskipun individu berada di lokasi dengan perlindungan data yang memadai, data tersebut berpotensi berakhir di negara-negara dengan kerangka hukum yang berbeda, atau bahkan di wilayah yang tidak memiliki regulasi sama sekali. Dengan demikian, apabila hak atas data pribadi dilanggar, individu tersebut berisiko tidak memperoleh pemulihan. Sehingga perlu diperhatikan bahwa teknologi yang tidak dimanfaatkan dengan baik akan berdampak buruk jika penggunaannya tidak terkontrol, dalam hal ini data pribadi tidak dilindungi (Tsamara, 2021).

Indonesia saat ini berada pada tahap revolusi industri 4.0, dimana teknologi komunikasi dan informasi banyak digunakan di sektor industri. Inovasi dan teknologi yang berkembang memiliki kemampuan untuk menyimpan dan menganalisis data guna memfasilitasi aktivitas manusia. Transformasi ini berdampak pada berbagai aspek kehidupan yang tidak terlepas dari teknologi, termasuk dalam penyelenggaraan *e-commerce* di sektor perdagangan, *mobile banking* dalam sektor perbankan, *online education* dalam sektor pendidikan, *e-government* untuk layanan pemerintah berbasis digital, media sosial (seperti Facebook, X, TikTok, dll) untuk interaksi sosial, mesin pencari seperti *Google*, serta *google maps* untuk pencarian informasi. Selain itu, terdapat pula berbagai bentuk penyimpanan data otomatis yang terhubung melalui perangkat seluler dengan metode *cloud* (Mahardika, 2021).

Semua aktivitas yang tercantum di atas memerlukan verifikasi identitas oleh pengontrol atau pemroses data. Langkah ini dilakukan untuk menjamin bahwa yang melakukan aktivitas elektronik tersebut bukanlah *bot*, melainkan manusia yang dapat dimintai pertanggungjawaban secara hukum. Kondisi ini menjadi dasar bagi pengontrol untuk mewajibkan setiap pengguna yang ingin menggunakan layanan memberikan data pribadinya, seperti nama, tempat dan tanggal lahir, alamat, kartu keluarga, nomor induk kependudukan, status

perkawinan, dan berbagai identitas lainnya, yang pada dasarnya merupakan informasi data pribadi. (Mahardika, 2021).

Teknologi informasi pada saat ini berperan sebagai “pedang bermata dua”, karena di satu sisi memberikan kontribusi terhadap peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sementara di sisi lain berfungsi juga sebagai sarana untuk melakukan tindakan melawan hukum yang cukup efektif seperti kejahatan di dunia maya, yang dikenal dengan istilah "*cybercrime*". *Cybercrime* yang diakibatkan oleh kebocoran data pribadi meliputi pornografi, perjudian, penipuan, hingga kejahatan internasional (perdagangan narkoba, mafia, terorisme, pencucian uang, perdagangan manusia) (Rumlus & Hartadi, 2020).

Regulasi perlindungan data pribadi yang dilemahkan dapat mengakibatkan pembatasan terhadap hak-hak individu yang berkaitan dengan informasi data pribadi. Namun, apabila regulasi mengenai perlindungan data pribadi diperkuat, individu akan memiliki lebih banyak hak terkait data pribadinya. Selanjutnya, tingkat kontrol yang dimiliki individu akan meningkat, sehingga mengurangi kemungkinan terjadinya penyalahgunaan data pribadi. Hal ini tidak hanya berlaku untuk perusahaan tertentu, tetapi juga mencakup pemerintah yang membatasi kontrol individu terhadap data pribadinya.

Pada Juli 2020, Mahkamah Eropa menolak kesepakatan antara perusahaan teknologi yang memungkinkan transfer data pribadi dari server yang berlokasi di Uni Eropa ke server di Amerika Serikat. Gugatan dalam kasus ini diajukan oleh Maximilian Schrems, seorang warga negara Austria, yang menuntut Komisi Perlindungan Data Pribadi Irlandia serta Facebook (Banyu, 2023). Dalam konteks ini, kesepakatan *Privacy Shield* memungkinkan terjadinya transfer data antar server. Isi gugatan menyatakan bahwa standar perlindungan data pribadi di Amerika Serikat lebih rendah dibandingkan dengan yang ada di Uni Eropa, disebabkan oleh kemungkinan akses data pribadi oleh lembaga intelijen, kurangnya pengawasan, serta tidak adanya mekanisme banding jika terjadi masalah pada data tersebut. Dalam putusannya, Mahkamah Eropa menekankan perlunya lembaga pengawas independen yang dapat menentukan dan mengatur mekanisme penyelesaian sengketa serta pemulihan hukum yang diperlukan. Kasus ini memiliki signifikansi yang tidak hanya bagi pihak-pihak yang terlibat, tetapi juga secara khusus penting untuk Indonesia. Sebab Kementerian Komunikasi dan Informatika (KOMINFO) berencana akan membentuk lembaga pengawas pelindungan data pribadi tahun 2024 (Iradat, 2024).

Teori Hukum internasional, diketahui bahwa “suatu data pribadi tunduk dibawah hukum dimana server dari data pribadi tersebut berada sehingga negara tujuan pengiriman data pribadi bisa saja merupakan suatu negara dengan kapasitas pelindungan data pribadi yang lemah, atau bahkan tidak memiliki pelindungan data

pribadi" (Lubis, 2021). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia telah berlaku. Namun hingga saat ini belum ada peraturan pelaksana yang mengatur tentang lembaga pelindungan atau pengawas data pribadi. Keberadaan lembaga ini sangat relevan mengingat tugasnya dalam pengawasan dan penegakan UU PDP.

Pelindungan data pribadi di Indonesia masih kurang kuat karena Indonesia belum mempunyai lembaga pengawas pelindungan data pribadi. Selain itu, penting untuk dilihat pula sejauh mana independensi dari Lembaga Pengawas Data Pribadi, yang dapat dibentuk dengan merujuk pada konsep ideal lembaga independen yaitu Konsep *Independent Regulatory Agencies* (IRAs).

Permasalahan kebocoran data pribadi di Indonesia tidak pernah terelakan. Pada bulan Mei tahun 2021, terdapat sebanyak 279 juta data pengguna BPJS Kesehatan dijual di situs forum *online* Raidforums.com. Kemudian pada tahun 2022, data SIM *card* milik masyarakat Indonesia dijual, hal tersebut diklaim sebagai ulah *hacker* Bjorka. Kabarnya, terdapat 1,3 miliar data pendaftar SIM *card*, NIK, nomor telepon penyedia, dan registrasi terkini sebanyak 87 GB. Adapun harga data ini dijual seharga Rp 743,5 juta. Terdapat 1,04 juta akun yang mengalami kebocoran data selama kuartal II pada tahun 2022 di Indonesia. Bahkan kebocoran data di internet pada kuartal II tersebut melonjak sebesar 143% dari quartal I tahun 2022 (Dhewa & Yossyafaat, 2023).

Tahun 2023 juga terjadi kasus kebocoran data yang melibatkan nasabah Bank Syariah Indonesia (BSI). Pada tanggal 8 Mei 2023, terdapat keluhan adanya gangguan layanan transaksi, sebelum data bocor. Lockbit berhasil mencuri 1,5 TB informasi data pribadi dalam kasus pencurian data nasabah BSI. Lockbit merupakan salah satu kelompok *ransomware* yang berasal dari negara Rusia. Pihak BSI sempat bernegosiasi dengan Lockbit. Lockbit meminta uang tebusan sebesar Rp.296 Miliar. Namun pihak BSI tidak menebusnya, karena tak kunjung ditebus pada 16 Mei 2023 Lockbit menyebarkan data tersebut ke pasar gelap (Widjaja & Cesarianti, 2024).

Banyaknya permasalahan terkait pelindungan data pribadi dan pentingnya percepatan pembentukan Lembaga Pengawas Data Pribadi di Indonesia, menjadi topik penelitian yang menarik untuk dikaji terkait bagaimana urgensi pembentukan Lembaga Pengawas Data Pribadi di Indonesia, selain itu bagaimana rekomendasi pembentukan Lembaga Pengawas Data Pribadi berdasarkan konsep *Independent Regulatory Agencies* (IRAs) di Indonesia sebagai upaya pelindungan hukum transfer data pribadi lintas negara. Pemerintah Indonesia dirasa perlu untuk segera membentuk Lembaga Pengawas Data Pribadi sebagaimana yang telah diamanatkan oleh UU PDP, pembentukan Lembaga Pengawas ini dibutuhkan agar

masyarakat dapat melaporkan dan mendapatkan pelindungan yang berkaitan dengan data pribadi di dunia maya.

Beberapa penelitian terdahulu terkait urgensitas pembentukan Lembaga Pengawas Data Pribadi telah ditemukan oleh penulis antara lain penelitian yang dilakukan oleh Nina Gumzej Tahun 2013 yang berjudul "*Selected Aspects of Proposed New EU General Data Protection Legal Framework And The Croatian Perspective".* Hasil penelitian menggambarkan peran penting otoritas perlindungan data pribadi di negara-negara Uni Eropa serta menggambarkan pentingnya lembaga tersebut untuk bersifat independen (Gumzej, 2013).

Penelitian lain yang dilakukan oleh Marta Claudia Cliza dan Laura Cristiana Spataru-Negura yang berjudul "*The General Data Protection Regulation: What Does The Public Authorities And Bodies Need To Know And To Do? The Rise Of The Data Protection Officer*". Hasil Penelitian menunjukkan bahwa independensi sangat penting bagi pegawai yang bertanggung jawab dalam menangani isu perlindungan data pribadi (Cliza & Spataru-Negura, 2018).

Penelitian oleh Rizky Pratama dan Evi Retno Wulan Tahun 2023 dengan judul "Urgensitas Pembentukan Lembaga Penyelenggaraan Pelindungan Data Pribadi". Hasil penelitian menunjukkan bahwa pembentukan penyelenggara perlindungan data pribadi merupakan respons terhadap kebutuhan masyarakat akan perlindungan data pribadi. Penyelenggara tersebut juga dapat dimanfaatkan oleh masyarakat untuk mengajukan keluhan atau menyampaikan aspirasi terkait perlindungan data pribadi. Oleh karena itu, lembaga yang ideal harus bersifat independen (Pratama & Wulan, 2023).

Penelitian lainnya yang dilakukan oleh Azza Fitrahul Faizah dkk Tahun 2023 yang berjudul "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan perbandingan hukum antara Hong Kong dan Singapura", penelitian menunjukkan bahwa keberadaan lembaga yang bersifat independen dapat memperkuat efektivitas hukum perlindungan data pribadi serta memenuhi standar kecukupan (*adequacy*) yang setara dengan negara-negara maju lainnya. Terdapat beberapa rekomendasi untuk membentuk model kelembagaan lembaga pengawas data pribadi, baik melalui otoritas pengawas tunggal (*single supervisory authority)* maupun model berbasis kementerian (*ministry based-models)* (Faizah et al., 2023).

Selanjutnya penelitian yang dilakukan oleh Gunawan Widjaja dan Fransiska Milenia Cesarianti Tahun 2024 yang berjudul "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". Hasilnya Mengkaji urgensi pembentukan Lembaga Pengawas Perlindungan Data Pribadi yang dapat menjalankan fungsi dan

kewenangannya di Indonesia. Pembentukan lembaga ini diharapkan dapat diwujudkan melalui produk Peraturan Presiden. Pemerintah diharapkan segera mendirikan Lembaga Pengawas yang memiliki kewenangan penuh terkait perlindungan data pribadi (Widjaja & Cesarianti, 2024).

Beberapa penelitian sebelumnya, terdapat kebaruan pada penelitian ini yaitu pada penelitian ini akan mengkaji terkait pentingnya pembentukan Lembaga Pengawas Data Pribadi dengan konsep *Independent Regulatory Agencies* (IRAs) di Indonesia sebagai upaya pelindungan hukum terhadap transfer data pribadi lintas negara.

B. METODE PENELITIAN

Jenis penelitian yang digunakan ialah penelitian hukum normatif, yang bertujuan untuk mengkaji hukum sebagai norma atau kaidah yang berlaku dalam masyarakat dan berfungsi sebagai acuan bagi perilaku individu (Ishaq, 2017). Penelitian ini menggunakan metode pendekatan undang-undang, yang bertujuan untuk mengkaji dan menganalisis semua peraturan perundang-undangan yang relevan dengan isu hukum yang sedang diteliti. Selain itu, pendekatan konseptual digunakan untuk menggali pandangan dan doktrin yang berkembang dalam ilmu hukum. Pendekatan perbandingan juga diterapkan dengan cara membandingkan berbagai peraturan perundang-undangan pada suatu negara dengan peraturan di negara lain yang membahas mengenai hal yang sama (Ishaq, 2017). Data dikumpulkan dengan menggunakan studi kepustakaan *(library research)* yang memfokuskan pada data sekunder, berupa bahan hukum primer yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan peraturan perundang-undangan lainnya yang ada kaitannya dengan penelitian, serta bahan hukum sekunder berupa literatur dan karya ilmiah yang terdapat kaitannya dengan penelitian. Penelitian dilaksanakan melalui pendekatan deskriptif analitis ialah dengan menggambarkan fakta hukum yang terjadi terkait pelindungan data pribadi lintas negara dan mengkajinya dengan membuat uraian secara sistematis faktual dan tepat berkaitan dengan pelindungan hukum terhadap transfer data pribadi lintas negara, serta pentingnya pembentukan Lembaga Pengawas Data Pribadi salah satunya dalam melindungi transfer data pribadi lintas negara yang dikaji dengan peraturan perundangan-undangan, yang kemudian hasil dari penelitian ini disusun secara runtut dan sistematis. Adapun teknik analisis data yang diterapkan adalah analisis kualitatif, berupa penguraian data yang telah diolah secara mendetail ke dalam format deskriptif.

C. HASIL DAN PEMBAHASAN

1. Urgensi Pembentukan Lembaga Pengawas Data Pribadi Independen di Indonesia

Internet telah berperan penting dalam menghubungkan komunikasi dan transfer data

pribadi antar negara. Seiring dengan meningkatnya transaksi lintas batas, jumlah negara yang mengadopsi perlindungan data pribadi juga bertambah, bersamaan dengan peningkatan infrastruktur internet. Hal ini menyebabkan kebutuhan akan *data protection officer* semakin meningkat (Yuniarti, 2022). Data pribadi kemudian dapat diproses untuk menghasilkan nilai ekonomi atau dimonetisasi, contohnya dengan membuat profil individu yang dapat digunakan untuk tujuan periklanan atau keperluan lainnya.

Menurut hasil survei APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) di Tahun 2024, presentasi pengguna internet di Indonesia mencapai 79.50% dengan kalkulasi 221.563.479 penduduk merupakan pengguna internet dari total keseluruhan 278.696.200 penduduk Indonesia pada Tahun 2023 (APJII, 2024). Berdasarkan jumlah tersebut, sekitar 79.50% dari pengguna internet di Indonesia menggunakan setidaknya satu *platform* media sosial. *Platform* media sosial yang menggunakan data pribadi paling banyak di Indonesia umumnya yang memiliki fitur-fitur interaktif dan personalisasi yang intensif. Berdasarkan data dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) tahun 2024, media sosial yang paling banyak penggunanya yaitu facebook dengan jumlah pengguna sebanyak 64,35% dari total populasi pengguna internet. Sisanya, Youtube 50,84%, Tiktok 34,36%, Instagram 29,68%, dan X 1,06%. Adapun media chat yang paling banyak penggunanya di Indonesia pada tahun 2024 yaitu WhatsApp sebanyak 97,86% dari total pengguna internet (APJII, 2024).

Platform-platform tersebut diatas mengumpulkan data pribadi seperti nomor telepon, kontak, foto, video, aktivitas pencarian dan lokasi pengguna untuk meningkatkan pengalaman komunikasi. Facebook dan WhatsApp merupakan *platform* media hasil karya perusahaan yang beroperasi di luar Indonesia, sehingga telah terjadi transfer data pribadi lintas negara dalam jumlah yang besar. Dengan besarnya angka pengguna internet oleh masyarakat di Indonesia, maka akan semakin rentan pula keamanan data pribadi yang disimpan, digunakan, maupun yang dikirimkan (transfer) ke pihak lainnya di *platform* digital. Selain itu aktivitas yang berjalan secara online juga memiliki risiko apabila data atau informasi tersebut mengalami kebocoran data dan digunakan dengan tidak semestinya oleh pihak-pihak yang tidak bertanggung jawab.

Transfer Data Pribadi adalah istilah yang menggambarkan pengelolaan data pribadi dalam bentuk pengiriman data pribadi di wilayah hukum suatu negara maupun ke luar wilayah hukum suatu negara yang dilakukan oleh pemilik data pribadi. Artinya bahwa pemilik data pribadi (subjek data pribadi) memiliki kewenangan untuk menentukan peruntukan data pribadi miliknya, salah satunya ialah melakukan transfer data pribadi (Dhewa & Yossyafaat, 2023). Pengaturan transfer data pribadi di Indonesia diatur melalui

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Transfer data pribadi dibedakan menjadi 2 (dua) bentuk, yaitu Transfer Data Pribadi dalam Wilayah Hukum Negara Republik Indonesia dan Transfer Data Pribadi ke Luar Wilayah Hukum Negara Republik Indonesia (*cross-border transfer*) (Sangojoyo, Kevin, & Sunlaydi, 2022).

Pengendali Data Pribadi berdasarkan draft Rancangan PP tentang Peraturan Pelaksanaan UU PDP, dapat melakukan transfer Data Pribadi kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi di luar wilayah hukum Negara Republik Indonesia. Transfer Data Pribadi tersebut memiliki kriteria: "a) dilakukan oleh Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; b) Pengendali Data Pribadi membuat Data Pribadi tersedia untuk Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima Data Pribadi; dan c) Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima Data Pribadi berada di luar wilayah hukum Negara Republik Indonesia." Dalam melakukan transfer Data Pribadi, Pengendali Data Pribadi yang melakukan transfer Data Pribadi dan yang menerima transfer Data Pribadi wajib melakukan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan di bidang Pelindungan Data Pribadi.

Ruang lingkup transfer data dapat dibedakan menjadi dua yaitu di dalam negeri atau di luar negeri. Ruang lingkup tersebut tetap mewajibkan keduanya mematuhi beberapa persyaratan yang ada. Untuk dapat melakukan transfer data dalam negeri maka data *controller* dan data *processor* wajib memastikan terjaminnya pelindungan data tersebut, tentunya disesuaikan dengan peraturan perundang-undangan yang berlaku di Indonesia. Sedangkan untuk ke luar negeri, data *controller* harus meminta persetujuan tertulis dari pemilik data pribadi.

Persyaratan transfer data ke luar negeri dilakukan berdasarkan persyaratan sebagai berikut (Thea, 2022): "a) Sebelum melakukan transfer data pribadi ke luar negeri, pengendali data pribadi wajib memastikan negara tempat pengendali data pribadi dan/atau prosesor data pribadi yang menerima transfer data itu punya tingkat pelindungan data pribadi yang setara atau lebih tinggi dari UU PDP di Indonesia; b) Jika negara tujuan yang menerima data itu tidak memiliki aturan yang setara atau lebih tinggi dari UU PDP, pengendali data pribadi wajib memastikan ada pelindungan data pribadi yang memadai dan bersifat mengikat. Bisa diartikan juga melalui kontrak atau instrumen yang mengikat, sehingga penerima data tunduk pada aturan di Indonesia; c) Jika kedua syarat tersebut tidak terpenuhi, pengendali data pribadi wajib mendapatkan persetujuan subjek data pribadi".

Apabila negara tempat kedudukan Pengendali Data Pribadi dan/ atau Prosesor Data Pribadi yang tidak memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari

yang diatur dalam UU PDP, tetap masih dapat melakukan transfer Data Pribadi dengan memastikan terdapat Pelindungan Data Pribadi yang bersifat mengikat dan memadai di negara yang menerima transfer Data Pribadi. Apabila tidak terdapat Pelindungan Data Pribadi yang bersifat memadai dan mengikat, tetap masih dapat melakukan Transfer Data ke luar wilayah Hukum Negara Republik Indonesia dengan mendapatkan persetujuan dari Subjek Data Pribadi. Jika terjadi pelanggaran terhadap ketentuan ini dikenai sanksi administratif.

Sebelum adanya UU PDP standar perlindungan data pribadi di Indonesia diterapkan melalui berbagai undang-undang. Beberapa peraturan perundang-undangan yang mengatur perlindungan data pribadi, antara lain Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan lain-lain (Setiawan & Najicha, 2022). Banyak peraturan perundang-undangan yang tidak sinkron satu sama lain, sehingga menciptakan kebingungan dalam implementasi dan kepatuhan terhadap perlindungan data pribadi. Hal ini mengakibatkan kesulitan bagi pelaku usaha dan individu dalam memahami kewajiban mereka. Tidak ada kerangka hukum yang komprehensif untuk seluruh sektor dalam pengelolaan data pribadi. Dengan disahkannya UU PDP, diharapkan dapat menjadi kerangka hukum yang lebih jelas dan komprehensif untuk melindungi data pribadi di Indonesia, mengurangi tumpang tindih regulasi, serta meningkatkan kesadaran masyarakat terkait pentingnya perlindungan data pribadi.

Data pribadi yang dikumpulkan oleh perusahaan teknologi dapat dikirimkan ke negara-negara di luar yurisdiksi hukum negara asal pengguna data pribadi. Dalam situasi seperti ini, pihak ketiga dapat menggunakan informasi data pribadi kita secara tidak tepat jika mereka tidak diawasi dengan benar. Sehingga pelindungan data pribadi menjadi penting untuk diberi perhatian lebih.

Sebelum pembentukan lembaga pengawas data pribadi di Indonesia, pengawasan terhadap data pribadi dilakukan melalui berbagai institusi yang ada, tidak ada lembaga khusus yang secara eksklusif dalam mengawasi data pribadi. Kementerian Komunikasi dan Informatika (KOMINFO) memiliki peran penting dalam mengatur dan mengawasi perlindungan data pribadi. Namun, kewenangannya terbatas dan tidak mencakup pengawasan independen terhadap pengelolaan data pribadi oleh sektor swasta dan publik. KOMINFO tidak optimal dalam melakukan investigasi dan pengawasan terkait dengan pelindungan data pribadi. Oleh karena itu, diperlukan reformasi hukum yang didampingi dengan rekonsepsi lembaga pengawas yang terkait dengan perlindungan data pribadi sebagai

unsur utama dalam penegakan hak privasi di era disrupsi, sesuai dengan ketentuan konstitusi (Juaningsih et al., 2021).

Otoritas Jasa Keuangan (OJK) dalam konteks sektor keuangan mengawasi lembaga keuangan yang juga berurusan dengan data pribadi nasabah. Namun, pengawasan ini lebih bersifat sektoral dan tidak menyeluruh tidak berjalan baik karena data nasabah perbankan sering kali dicuri (Sandi, 2019). Lembaga perlindungan konsumen juga terlibat dalam isu-isu terkait privasi dan perlindungan data, tetapi tidak memiliki kekuatan hukum untuk menindaklanjuti pelanggaran secara langsung. Adapun dalam penegakan hukum terkait dengan pelanggaran data pribadi yang dilakukan oleh kepolisian, tetapi ini lebih bersifat reaktif terhadap insiden tertentu daripada pengawasan proaktif. Permasalahan dalam pengawasan/pemantauan data pribadi yang sebelumnya bersifat sektoral dalam implementasinya dikatakan tidak berjalan dengan baik (Doly, 2021).

Tanpa lembaga khusus terdapat tantangan dalam koordinasi antara berbagai institusi yang memiliki tanggung jawab terhadap perlindungan data pribadi. Lembaga-lembaga yang ada sering kali terpengaruh oleh kepentingan politik atau sektoral, sehingga independensi dalam pengawasan sulit dicapai. Di Indonesia sebelum adanya UU PDP kerangka hukum untuk melindungi data pribadi masih sangat terbatas, sehingga banyak insiden pelanggaran tidak dapat ditindaklanjuti secara efektif. Untuk menindaklanjuti amanat dari UU PDP terkait pembentukan lembaga pengawas yang independen diharapkan dapat memenuhi kebutuhan akan pengawasan yang efektif dan akuntabel terhadap perlindungan data pribadi.

Pelindungan data pribadi telah diamanatkan dalam Pasal 28G ayat (1) UUD NRI Tahun 1945 yang menyatakan bahwa “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Diatur juga dalam Pasal 28H ayat (4) yang menyatakan bahwa “Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun”. Sesuai dengan ketentuan Pasal tersebut, negara berkewajiban untuk memberikan upaya perlindungan kepada setiap orang, termasuk perlindungan jiwa dan tubuh seseorang, serta apa yang dimiliki setiap orang, termasuk informasi data pribadi.

Definisi yang signifikan dalam regulasi perlindungan data pribadi adalah "pemrosesan data pribadi". Secara umum, pemrosesan data pribadi diartikan sebagai seluruh rangkaian tindakan yang berkaitan dengan data pribadi, termasuk tetapi tidak terbatas pada pengumpulan, pencatatan, pengorganisasian, penyimpanan, modifikasi, penggunaan, pengungkapan, pembatasan, penghapusan data

pribadi; serta/atau transfer data pribadi antar negara (*transborder personal data transfer*) (Sirie, 2021).

Peraturan Perlindungan Data Pribadi di Benua Eropa khususnya di Negara Jerman, sebelum penerapan EU GDPR (*European Union General Data Protection Regulation)*, Jerman memiliki kerangka hukum tersendiri yang mengatur perlindungan data pribadi, yaitu Undang-Undang Perlindungan Data Federal Jerman, yang dikenal sebagai *Bundesdatenschutzgesetz* (BDSG). Undang-undang ini mengatur secara rinci mengenai pemrosesan data, baik dalam konteks umum maupun dalam konteks yang lebih sensitif atau rahasia. BDSG berfungsi untuk memperjelas dan melengkapi ketentuan-ketentuan GDPR, menyesuaikan dengan konteks hukum dan sosial di Jerman, serta menetapkan hak-hak individu terkait perlindungan data pribadi mereka (Anjawai, Amboro, & Hutauruk, 2022). Jerman barat juga mengeluarkan *The Data Protection Act of the State of Hesse*, merupakan undang-undang awal yang muncul terkait privasi dan keamanan data dan dijadikan dasar panduan. Dibentuk oleh OECD (*Organization for Economic Cooperation and Development)* untuk pelindungan privasi setiap individual secara lintas negara. Ini juga merupakan aksi multinasional pertama yang membatasi kemampuan perusahaan multinasional untuk mentransmisi data secara internasional (Tumindak, Ramadhiani, & Vivian, 2020). Jerman memiliki Dewan Perlindungan Data Eropa (*European Data Protection Board*/EDPB) yang merupakan badan resmi yang dibangun khusus wilayah Uni Eropa (UE). Setiap negara memiliki tanggungjawab menunjuk satu supervise yang ditugaskan untuk memantau dalam mengimplementasikan norma dan peraturan dalam GDPR. Dewan Perlindungan ini juga bertanggungjawab menindaklanjuti permasalahan apabila terjadi pelanggaran dalam Perlindungan Data Pribadi (Anjawai, Amboro, & Hutauruk, 2022). EDPB sebagai organ independen, tidak bertanggung jawab kepada siapapun, namun wajib berkoordinasi dengan Komisi Eropa dan otoritas perlindungan data nasional untuk mencapai tujuan perlindungan data yang konsisten di seluruh wilayah UE.

Berkaca pada negara lain yaitu negara Inggris, pedoman Inggris tentang perlindungan data pribadi dirinci dalam *The Data Protection Act* 1998 (Undang-Undang Perlindungan Data 1998) (Latumahina, 2014). Dalam isi undang-undangnya menyebutkan suatu badan pelaksana yaitu *Information Commissioner's Office* (ICO) memiliki wewenang dalam pengawasan terhadap pengguna data yang berkuasa atas data pribadi (Sautunnida, 2018). *Information Commissioner's Office* (ICO) di Inggris adalah lembaga pengawas independen yang bertanggung jawab kepada Parlemen Britania Raya. Secara spesifik, ICO dipilih dan dilantik oleh Parlemen. Undang-Undang Perlindungan Data Pribadi di Inggris membatasi denda untuk pelanggaran pada 500.000 GBP (Wolff & Atallah, 2021).

Perlindungan data pribadi di Inggris diatur dengan ketat melalui regulasi yang ada, yang mencakup larangan untuk transfer data pribadi ke luar wilayah Eropa tanpa adanya jaminan perlindungan yang memadai. Inggris tidak mengizinkan pengalihan atau penyediaan data pribadi ke negara lain untuk tujuan apa pun, meskipun dilakukan secara legal, jika negara tujuan tersebut tidak memiliki undang-undang yang khusus mengatur perlindungan data pribadi (Rizal, 2019).

Pentingnya penggunaan data pribadi tidak terbatas pada sektor swasta, tetapi juga mencakup sektor publik. Oleh karena itu, lembaga pengawas menjadi isu sentral di berbagai negara. Hal ini dilakukan juga mengingat adanya ketentuan dalam regulasi di Inggris yang bersifat tegas melarang transfer data pribadi untuk dilakukan ke luar negara Eropa, kecuali negara yang bersangkutan dapat menjamin kesetaraan pelindungan data. Pemberlakuan tersebut dikenal dengan *adequacy principle* sesuai ketentuan GDPR. Implikasi dari adanya prinsip tersebut adalah jika negara di luar Uni Eropa belum memiliki pengaturan spesifik terkait pelindungan data pribadi, maka negara terkait tidak memiliki kewajiban bahkan melarang adanya transfer data pribadi lintas negara (Rizal, 2019). Berkaitan dengan hal ini pula, sudah seharusnya pemerintah Indonesia hendaknya segera membentuk Lembaga Pengawas Data Pribadi yang independen, mengingat transfer data di lingkup transnasional pada era globalisasi saat ini masif dilakukan.

Beberapa contoh yang relevan dari *General Data Protection Regulation* (GDPR) meliputi dasar hukum (legal basis) pemrosesan data, analisis dampak perlindungan data, serta desain privasi. Konsep-konsep ini sangat cocok untuk diterapkan di Indonesia karena mereka tidak hanya berfokus pada perlindungan data tetapi juga mencegah kebocoran data. Selain itu, GDPR tidak hanya mengatur tindakan pasca-pelanggaran perlindungan data, tetapi juga mendorong preventifitas insiden-insiden serupa. Oleh karena itu, Indonesia dapat mengintegrasikan konsep-konsep ini ke dalam regulasinya.

Negara di Asia Tenggara yaitu Malaysia, juga telah memiliki aturan khusus Pelindungan Data Pribadi. Aturan tersebut tertuang dalam *Personal Data Protection Act* (PDPA) 2010 serta memiliki Lembaga pengawas data pribadi yang bernama Pesuruhjaya Perlindungan Data Peribadi (*Personal Data Protection Commissioner*), lembaga tersebut bertanggung jawab kepada Menteri. Peraturan Perlindungan Data Pribadi (PDPA) di Malaysia bertujuan untuk mengatur pengelolaan data pribadi dalam konteks transaksi komersial oleh pengguna data, serta untuk melindungi kepentingan subjek data pribadi. Tujuan ini hanya dapat dicapai melalui persetujuan yang jelas dari individu yang bersangkutan, yang harus diperoleh sebelum proses pengolahan data dilakukan. Selain itu,

individu juga diberikan hak untuk mengakses dan mengontrol pengolahan data pribadi mereka secara efektif. PDPA menetapkan bahwa pengolahan data pribadi harus dilakukan dengan memperhatikan prinsip-prinsip tertentu, termasuk keabsahan, kebutuhan, dan tidak melebihi batasan yang ditetapkan. Persetujuan dari subjek data harus diperoleh sebelum pengumpulan dan pemrosesan data dilakukan, serta pengguna data wajib memberikan informasi yang jelas mengenai tujuan pengumpulan tersebut. Selanjutnya, subjek data berhak untuk mengakses, mengubah, dan membatasi penggunaan data pribadinya sesuai dengan peraturan yang berlaku. Hal ini identik dengan apa yang tercantum dalam Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Indonesia (UU ITE) (Sautunnida, 2018). PDPA menyatakan bahwa tidak boleh ada transfer data pribadi ke tempat-tempat di luar Malaysia; setiap transfer hanya dapat dilakukan jika diizinkan dan ditentukan oleh Menteri Penerangan, Kebudayaan, dan Komunikasi. Selain itu, negara tujuan di mana data dikirimkan harus memenuhi tingkat perlindungan yang cukup baik, atau setidaknya tingkat perlindungan yang sama dengan yang telah diberlakukan di bawah PDPA Malaysia (Matheus & Gunadi, 2024).

Singapura memberlakukan *Personal Data Protection Act* (PDPA**)** pada tahun 2012, PDPA mengatur akuisisi (pengumpulan), pengungkapan, dan penggunaan data pribadi di Singapura. Singapura juga mempunyai lembaga yang dikenal sebagai *Personal Data Protection Commission* (PDPC) bertanggung jawab kepada Menteri Komunikasi dan Informasi. PDPC ini menghasilkan regulasi dan panduan yang relevan dengan pelaku usaha atau pihak yang mengumpulkan data di Singapura (KlikLegal, 2021). Di Singapura, pihak yang mengumpulkan data harus meminta persetujuan individu sebelum mengumpulkan atau menggunakan data pribadi. PDPA mengharuskan organisasi untuk memastikan bahwa data pribadi yang ditransfer ke luar negeri dilindungi dengan cara yang setara dengan perlindungan yang diberikan di Singapura. Adapun terkait sanksi, pelanggaran terhadap PDPA dapat dikenakan denda hingga SGD 1 juta.

Hong Kong merupakan entitas pertama di Asia yang menyediakan kerangka regulatif untuk perlindungan privasi data pribadi, yakni *Personal Data Privacy Ordinance* (PDPO) tahun 1995, yang telah dialami modifikasi signifikan pada tahun 2012. Lembaga khusus penanganan isu privasi data pribadi di Hongkong bernama *Privacy Commisioner for Personal Data* (PCPD), yang bertanggung jawab langsung kepada *Chief Executive*. Prinsip perlindungan hak privasi data pribadi di Hong Kong mencakup sejumlah ketentuan yang mengatur pengumpulan data, yaitu: pengumpulan data harus dilakukan dengan tujuan yang sah dan sesuai dengan kepentingan pengumpul; penggunaan dan pengungkapan data pribadi harus konsisten dengan tujuan

pengumpulan serta memerlukan persetujuan dari pemilik data; kualitas data pribadi harus akurat dan terkini; penyimpanan data oleh pihak ketiga dibatasi dalam waktu; pengelola data pribadi wajib melindungi data dari akses yang tidak sah; dan transparansi mengenai penggunaan data oleh pihak ketiga diharuskan, yang mencakup kewajiban untuk mempublikasikan kebijakan privasi. Pelanggaran terhadap ketentuan ini dapat mengakibatkan tindakan hukum berupa somasi dari pemerintah Hong Kong kepada pihak yang bersangkutan (Tsamara, 2021).

Jepang sudah memberlakukan *Act on the Protection of Personal Information* (APPI) sejak tahun 2003. Terdapat sebuah badan administratif independen bernama *Personal Information Protection Commission* (PPC), yang bertanggung jawab kepada Parlemen Jepang. Amandemen terbaru APPI pada tahun 2020 memperkenalkan peraturan tambahan tentang transfer informasi lintas batas. Perusahaan yang tunduk pada ruang lingkup hukum Jepang harus mendapatkan persetujuan dari individu yang bersangkutan sebelum mentransfer data pribadi mereka ke luar Jepang. Sebagai bagian dari sistem perlindungan data pribadi, perusahaan yang mentransfer informasi pribadi ke luar Jepang harus menandatangani kontrak dengan entitas penerima di negara asing. Hal ini memberikan jaminan kepatuhan terhadap langkah-langkah keamanan dan perlindungan data, yang tercantum dalam kontrak, dan sesuai dengan persyaratan APPI. Jika informasi pribadi ditransfer lagi ke pihak ketiga di negara asing, PIC asal harus memastikan bahwa pihak ketiga tersebut mematuhi langkah-langkah keamanan dan privasi PIC dan pihak asli. Adapun terkait sanksi, pelanggaran terhadap APPI dapat mengakibatkan denda dan tindakan hukum lainnya.

Hal-hal positif yang dapat dicontoh oleh Negara Indonesia dalam membentuk Lembaga Pengawas Data Pribadi berdasarkan Lembaga Pengawas Data Pribadi dari berbagai negara yang telah disebutkan diatas ialah:

1. Independensi

   Lembaga yang telah disebutkan diatas beroperasi secara independen dari pemerintah dan sektor swasta, yang memungkinkan untuk membuat keputusan berdasarkan kepentingan publik tanpa campur tangan dari pihak-pihak lain. Lembaga harus bersifat independen dan tidak dipengaruhi oleh kepentingan institusi manapun.
2. Penegakan Hukum yang Tegas:

   Penegakan hukum yang tegas dalam konteks lembaga pengawas data pribadi sangat penting untuk memastikan perlindungan data individu dan kepatuhan terhadap regulasi.
3. Kerja sama Internasional

   Guna memastikan standar perlindungan data yang konsisten di seluruh dunia dapat setara dengan yang ada di Indonesia, maka lembaga pengawas data pribadi yang akan dibentuk nantinya harus aktif dalam menjalin koordinasi dengan lembaga negara lain. Kerja Sama Internasional dapat dilakukan dalam bidang

penegakan hukum (*mutual legal asistance*), pertukaran informasi, pengembangan kapasitas, sosialisasi, dan kegiatan lain terkait dengan Pelindungan Data Pribadi.

Beberapa penerapan prinsip-prinsip dalam EU GDPR patut diperhatikan seperti *Data Protection by Design* dan *by Default*. Prinsip ini mengadopsi prinsip-prinsip *Privacy by Design* yang ada pada ketentuan sebelumnya. Dalam EU GDPR, *Data Protection by Design* diartikan bahwa organisasi atau instansi sejak tahap awal harus mendesain pemrosesan data dengan menerapkan langkah teknis yang nantinya dapat terintegrasi dengan pengamanan yang diperlukan guna memenuhi persyaratan yang diatur dan melindungi hak dari subjek data.

Prinsip *Data Protection by Default* mengharuskan organisasi atau institusi untuk menjamin bahwa pengolahan data pribadi dilakukan dengan tingkat perlindungan privasi yang optimal. Hal ini berarti bahwa secara default, akses terhadap data pribadi harus dibatasi untuk tujuan tertentu dan tidak dapat diakses oleh pihak yang tidak berwenang. Oleh karena itu, aspek penting yang perlu diperhatikan adalah perlunya penjelasan yang jelas mengenai hak-hak subjek data dalam konteks tersebut. Beberapa kewajiban yang termaktub dalam prinsip tersebut di atas seyogyanya diatur lebih rigid dan komprehensif dalam regulasi turunannya yaitu melalui peraturan pemerintah yang telah diamanatkan oleh UU PDP.

Penting bagi Pemerintah Indonesia untuk segera mendirikan Lembaga Pengawas Data Pribadi sebagai langkah untuk memberikan perlindungan hukum terhadap transfer data pribadi antarnegara. Indonesia tidak hanya perlu mengadopsi regulasi perlindungan data yang telah terbukti efektif di berbagai belahan dunia, tetapi juga harus mempersiapkan langkah-langkah lanjutan setelah adopsi tersebut. Oleh karena itu, sangat krusial bagi Indonesia untuk dapat melaksanakan Undang-Undang Perlindungan Data Pribadi (UU PDP) di masa mendatang dan merumuskan peraturan turunan yang dapat berfungsi sebagai pedoman praktis bagi entitas yang melakukan pengumpulan data. Hal ini diperlukan untuk memastikan bahwa data pribadi yang ditransfer ke negara lain mendapatkan perlindungan yang memadai, setara dengan perlindungan yang diberikan di negara asal. Situasi yang harus dihindari adalah ketika negara penerima memiliki standar perlindungan data pribadi yang rendah atau bahkan tidak ada sama sekali, karena hal ini berpotensi menyebabkan penyalahgunaan data pribadi secara bebas. Tanpa adanya regulasi yang memadai terkait transfer data pribadi lintas negara, terdapat risiko bahwa individu atau entitas tertentu dapat memanfaatkan celah hukum untuk mengirim dan menyimpan data pribadi di negara-negara dengan standar perlindungan data yang rendah atau tanpa perlindungan sama sekali, sehingga terhindar dari

ketentuan perlindungan data yang berlaku di negara asal.

Lembaga pengawas data pribadi nantinya akan mengawasi pengelolaan data pribadi oleh penyelenggara sistem elektronik baik dari pemerintah maupun swasta, ini bisa memastikan adanya transparansi dan akuntabilitas dalam operasional data pribadi. Lembaga pengawas data pribadi juga memiliki tanggung jawab untuk memfasilitasi penyelesaian sengketa di luar pengadilan terkait pelanggaran UU PDP. Ini membantu mempercepat proses penanganan terkait permasalahan keamanan data di Indonesia.

2. Rekomendasi Pembentukan Lembaga Pengawas Data Pribadi Berdasarkan Konsep *Independent Regulatory Agencies* (IRAs) di Indonesia sebagai Upaya Pelindungan Hukum Transfer Data Pribadi Lintas Negara

Sebelum diberlakukannya UU PDP (Undang-Undang Perlindungan Data Pribadi), di Indonesia pengaturan mengenai perlindungan data pribadi tersebar diberbagai peraturan perundang-undangan (Ramadhani, 2022) yang bersifat sektoral dan terkait dengan isu tertentu, serta tidak semua regulasi tersebut mencakup pengaturan tentang transfer data pribadi lintas negara. Ketentuan mengenai transfer data pribadi lintas negara diatur dalam PP (Peraturan Pemerintah) No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP *E-Commerce*). Berdasarkan Pasal 59 ayat (2) huruf (h) *PP E-Commerce*, pengiriman data pribadi ke negara atau wilayah di luar Indonesia dilarang kecuali negara atau wilayah tersebut telah dinyatakan oleh Menteri Perdagangan memiliki standar dan tingkat perlindungan yang setara dengan Indonesia. Namun, sejak regulasi ini disahkan pada tahun 2019, Menteri Perdagangan belum menetapkan daftar negara-negara yang memenuhi kriteria tersebut, sehingga menciptakan ketidakpastian hukum bagi pelaku usaha di sektor e-commerce, terutama ketika diperlukan penggunaan layanan komputasi awan untuk pemrosesan data, yang umumnya beroperasi di luar negeri (Sirie, 2021).

Sebelum pembentukan lembaga pengawas data pribadi, Pasal 15 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur tentang lembaga yang memproses data pribadi secara elektronik dengan istilah Penyelenggara Sistem Elektronik (PSE). PSE merujuk pada entitas yang dapat berupa negara, badan usaha, atau masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik, baik secara individu maupun kolaboratif, untuk kepentingan mereka sendiri dan/atau pihak lain. PSE diwajibkan untuk menyelenggarakan sistem elektronik dengan cara yang andal, aman, dan bertanggung jawab. Selain itu, PSE memiliki tanggung jawab atas penyelenggaraan sistem elektronik yang mereka kelola dan juga bertanggung jawab jika terjadi kebocoran data pribadi pengguna. Namun, dari adanya aturan Penyelenggara Sistem Elektronik (PSE) di

Indonesia timbul bentuk-bentuk problem hukum yaitu kebebasan berpendapat yang dibatasi, pemblokiran konten (pembatasan akses), dan pelanggaran privasi (Sahib, Idayanti, & Rahayu, 2023).

Lembaga Pengawas Data Pribadi yang akan direkomendasikan penulis yaitu lembaga yang mengacu pada konsep ideal lembaga negara independen yang sejalan dengan syarat independensi lembaga dalam ketentuan EU GDPR (*European Union General Data Protection Regulation)*. Lembaga independen yang dibentuk merupakan lembaga negara di mana keanggotaannya berasal dari unsur non-negara dan diberi kewenangan serta pembiayaan dari anggaran negara. Realisasi keberadaan Lembaga Pengawas Data Pribadi di Indonesia merupakan unsur penting menjamin terlaksananya UU PDP. Lembaga Pengawas Pelindungan Data Pribadi ini dapat bekerja menjalankan fungsinya dalam hal pelindungan data pribadi dan menjamin kepatuhan para pengendali dan processor data pribadi baik dari individu, lembaga publik, maupun, badan privat.

Lembaga Pengawas Data Pribadi dapat dibentuk didasarkan pada konsep *Independent Regulatory Agencies* (IRAs). Pengertian konsep IRAs, merujuk pada makna konsep IRAs yang diperkenalkan oleh Rizki Ramadani dalam penelitiannya yang dibagi menjadi dua indikator yaitu pertama, independensi formal yang mengacu pada peraturan perundang-undangan terdiri dari independensi personalia, independensi fungsional, dan independensi institusional. Kedua, independensi *de facto* yang mengacu pada lembaga negara independen pada saat melaksanakan kewenangannya. Terdapat tiga aspek utama dari Konsep *Independent Regulatory Authorities* (IRAs), yaitu: pertama, independensi dari pejabat-pejabat terpilih; kedua, interaksi dengan lembaga administratif lainnya; dan ketiga, mekanisme pengambilan keputusan. Adapun konsep IRAs telah digunakan dibeberapa bentuk lembaga independen yang ada di Indonesia seperti KPU (Komisi Pemilihan Umum), OJK (Otoritas Jasa Keuangan), dan Ombudsman (Ramadani, 2020).

Konsep IRAs dianggap mampu untuk menyeimbangkan peran antara sektor administrasi publik, organisasi masyarakat sipil, dan warga negara. Lembaga ini akan diberikan kewenangan yang berdiri sendiri sehingga keberadaannya akan terpisah dari badan publik lainnya bahkan kementerian. Dimaksudkan untuk meminimalisasi intervensi kewenangan lembaga lain dalam melakukan penegakan hukum dan pengawasan terkait pelindungan data pribadi mengingat transfer data pribadi lintas negara kian meningkat. Adapun tugas khusus Lembaga Pengawas Data Pribadi ini singkatnya akan mengawasi dan menegakkan penerapan hukum pelindungan data pribadi secara optimal.

Pasal 58 ayat (4) UU PDP mengamanatkan bahwa "Lembaga sebagaimana bertanggung jawab kepada Presiden". Jadi nantinya, lembaga pengawas data pribadi akan bertanggung jawab

langsung kepada Presiden RI. Berdasarkan Pasal 59 UU PDP dikatakan bahwa lembaga melaksanakan: "a) Pengembangan dan penetapan kebijakan serta strategi Perlindungan Data Pribadi yang berfungsi sebagai panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi; b) pengawasan terhadap implementasi Perlindungan Data Pribadi; c) penegakan hukum administratif terhadap pelanggaran ketentuan Undang-Undang ini; dan d) fasilitasi penyelesaian sengketa di luar jalur peradilan".

Wewenang Lembaga Pengawas Data Pribadi berdasarkan Pasal 60 UU PDP, Lembaga berwenang untuk: "a) Merumuskan dan menetapkan kebijakan di bidang Pelindungan Data Pribadi; b) Melakukan pengawasan terhadap kepatuhan Pengendali Data Pribadi; c) Menjatuhkan sanksi administratif atas pelanggaran Pelindungan Data Pribadi yang dilakukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi; d) Membantu aparat penegak hukum dalam penanganan dugaan tindak pidana Data Pribadi sebagaimana dimaksud dalam Undang-Undang ini; e) Bekerja sama dengan lembaga Pelindungan Data Pribadi negara lain dalam rangka penyelesaian dugaan pelanggaran Pelindungan Data Pribadi lintas negara; f) Melakukan penilaian terhadap pemenuhan persyaratan transfer Data Pribadi ke luar wilayah hukum Negara Republik Indonesia; g) Memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada Pengendali Data Pribadi dan/ atau Prosesor Data Pribadi; h) Melakukan publikasi hasil pelaksanaan pengawasan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; i) Menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran Pelindungan Data Pribadi; j) Melakukan dan atas pengaduan, laporan, dan/atau hasil pengawasan terhadap dugaan terjadinya pelanggaran Pelindungan Data Pribadi; k) Memanggil dan menghadirkan Setiap Orang dan/atau Badan Publik yang terkait dengan dugaan pelanggaran Pelindungan Data Pribadi; l) Meminta keterangan, data, Informasi, dan dokumen dari Setiap Orang dan/ atau Badan Publik terkait dugaan pelanggaran Pelindungan Data Pribadi; m) Memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaan pelanggaran Pelindungan Data Pribadi; n) Melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga; dan o) Meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa Pelindungan Data Pribadi".

Lembaga Pengawas Data Pribadi berwenang memberikan sanksi administratif jika terjadi penyalahgunaan terhadap data pribadi. Sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan

data pribadi, penghapusan atau pemusnahan data pribadi; dan/atau denda administratif. Nantinya, sesuai dengan Pasal 57 ayat 3 UU PDP, "denda administratif tersebut paling tinggi 2 persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi denda administratif akan diatur dalam Peraturan Pemerintah". Terdapat juga ketentuan pidana pada UU PDP yaitu dalam Pasal 67 ayat (1) sampai dengan ayat (3), "untuk pidana penjara paling lama 5 Tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)".

Penegakan hukum oleh Lembaga Pengawas Data Pribadi, harus memiliki penegakan hukum preventif dan represif. Penegakan preventif yang dimiliki Lembaga Pengawas Data Pribadi yaitu kewajiban penyelenggara data untuk memberi laporan tahunan atas kinerja yang dilakukan oleh penyelenggara data yang berkaitan dengan data pribadi yang dikelola. Sedangkan penegakan represif yaitu dengan menerima aduan dari subjek data yang merasa dirugikan dari adanya pengelolaan data pribadi oleh pihak swasta maupun pihak badan publik. Hal ini dilakukan mengingat lembaga ini memiliki kewenangan melakukan investigasi pelanggaran data pribadi yang didasarkan dari adanya aduan subjek data yang merasa hak pelindungan data pribadinya dilanggar oleh penyelenggara data. Pelanggaran data pribadi dapat dilihat apabila penyelenggara data melanggar kewajibannya sebagaimana ketentuan di dalam UU PDP.

Penyelesaian sengketa yang akan dilakukan oleh Lembaga Pengawas Data Pribadi mengutamakan Mediasi. Mediasi dilakukan dalam jangka waktu paling lama 30 (tiga puluh) hari terhitung sejak pertemuan pertama Mediasi serta dapat diperpanjang berdasarkan kesepakatan Para Pihak yang bersengketa. Putusan dari ajudikasi non litigasi tersebut nantinya memuat sanksi administrasi dan/atau denda yang berkekuatan hukum setara dengan putusan pengadilan. Apabila ditemukan indikasi pelanggaran, maka lembaga dapat berwenang untuk membentuk majelis kemudian memanggil para pihak penyelenggara data untuk melakukan mediasi secara musyawarah mufakat. Tetapi, jika ternyata tidak dicapai mufakat dan mediasi dinyatakan gagal, maka dilanjutkan dengan proses litigasi non ajudikasi. Proses tersebut dilakukan untuk membuktikan ada atau tidaknya pelanggaran data pribadi yang dilakukan dengan mendatangkan saksi dan menyerahkan alat bukti terkait.

Setelah penyelenggara data dinyatakan melanggar, maka lembaga akan mengeluarkan putusan yang kekuatannya setara dengan putusan pengadilan disertai pemberian sanksi administrasi berupa pencabutan izin penyelenggara data untuk melakukan kegiatan yang berkaitan dengan data pribadi (seperti mengolah, mengambil, memproduksi, dan mendistribusi). Apabila ternyata penyelenggara

data merasa keberatan dengan putusan lembaga, maka penyelenggara data dapat menyampaikan sengketa terkait ke PTUN (Pengadilan Tata Usaha Negara) atas putusan terkait. Namun, jika dalam investigasi ditemukan adanya tindak pidana lain yang menyertai pelanggaran data pribadi tersebut maka lembaga berwenang untuk memberikan rekomendasi dan menyerahkan hasil investigasi sebagai alat bukti kepada Kejaksaan Agung untuk diselesaikan secara hukum acara pidana di lingkup Peradilan Umum.

Selain penegakan hukum dalam yurisdiksi nasional, Lembaga Pengawas Data Pribadi juga berwenang untuk menyelesaikan sengketa pelanggaran data pribadi apabila pelanggaran berkaitan dengan yurisdiksi negara lain atau dalam hal ini terdapat pelanggaran data pribadi lintas negara. Jika terjadi pelanggaran dengan negara lain, maka negara yang memiliki tingkat pelindungan data pribadi lebih kuat berhak untuk melaksanakan yurisdiksinya. Namun, jika yang melakukan pelanggaran memiliki tingkat pelindungan yang setara dengan Indonesia, maka yurisdiksi negara yang berhak menyelesaikan sengketa diakomodasi dari hasil kesepakatan bersama. Lembaga Pengawas Data Pribadi memiliki wewenang untuk menjalin kerja sama dengan negara lain berkaitan dengan perlindungan data pribadi, dalam rangka pelaksanaan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang dilaksanakan sesuai dengan ketentuan prinsip-prinsip hukum internasional dan peraturan perundang-undangan yang ada.

D. SIMPULAN

Pada Tahun 2024, presentase pengguna internet di Indonesia mencapai 79.50% dengan kalkulasi 221.563.479 jiwa merupakan pengguna internet dari total penduduk 278.696.200 jiwa. Setidaknya dari jumlah pengguna internet 79.50% di Indonesia menggunakan satu platform media sosial yang memerlukan data pribadi. Di Indonesia Tahun 2024, media sosial yang paling banyak penggunanya yaitu *facebook* sejumlah 64,35% dari total populasi pengguna internet. Adapun media chat yang paling banyak penggunanya yaitu *WhatsApp* sebanyak 97,86% dari total pengguna internet. Facebook dan WhatsApp merupakan *platform* media hasil karya perusahaan yang beroperasi di luar Indonesia, sehingga telah terjadi transfer data pribadi lintas negara dalam jumlah yang besar. Oleh karena itu, pembentukan Lembaga Pengawas Data Pribadi di Indonesia sangat penting untuk segera dibentuk guna meningkatkan efektivitas pelindungan transfer data pribadi, mengingat transfer data pribadi di lingkup transnasional pada era globalisasi saat ini masif dilakukan. Untuk mengatasi permasalahan yang timbul dari adanya transfer data pribadi dalam negeri dan luar negeri, juga diperlukan persyaratan khusus yang menjamin pelindungan data pribadi.

Pemerintah indonesia dapat mencontoh hal-hal positif dalam pembentukan lembaga

pengawas data pribadi negara lain yang sekiranya dapat dijadikan preseden untuk pembentukan Lembaga Pengawas Data Pribadi. Rekomendasi pembentukan Lembaga Pengawas Data Pribadi di Indonesia berdasarkan konsep *Independent Regulatory Agencies* (IRAs), yaitu pertama, independensi formal berdasarkan pada peraturan perundang-undangan yang terdiri dari independensi personalia, independensi fungsional, dan independensi institusional. Kedua, independensi *de facto* yang mengacu pada lembaga negara independen pada saat melaksanakan kewenangannya. Konsep IRAs dipilih karena telah diterapkan pada lembaga independen di Indonesia seperti KPU (Komisi Pemilihan Umum), OJK (Otoritas Jasa Keuangan), dan Ombudsman.

Lembaga Pengawas Data Pribadi akan bertanggung jawab langsung kepada Presiden, sesuai dengan amanat Pasal 58 ayat (4) Undang-Undang Perlindungan Data Pribadi (UU PDP). Berdasarkan Pasal 59 UU PDP, lembaga ini akan "melaksanakan perumusan dan penetapan kebijakan serta strategi Perlindungan Data Pribadi yang berfungsi sebagai panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi; melakukan pengawasan terhadap pelaksanaan Perlindungan Data Pribadi; menegakkan hukum administratif terhadap pelanggaran yang terjadi; serta memfasilitasi penyelesaian sengketa di luar jalur peradilan".

Lembaga Pengawas Data Pribadi diharapkan dapat menjamin terlaksananya UU PDP dengan melaksanakan fungsi pengawasan, penegakan hukum, terkait pelindungan data pribadi baik dalam negeri maupun luar negeri. Lembaga ini juga memiliki kewenangan untuk menyelesaikan sengketa pelanggaran data pribadi lintas negara dan melakukan kerja sama dengan negara lain terkait pelindungan data pribadi. Dalam penegakan hukumnya, diharapkan mampu untuk memberikan pelindungan terhadap transfer data pribadi lintas negara.

DAFTAR PUSTAKA

JURNAL

Anjawai, Namrysilia Buti., Amboro, Yudhi Priyo., & Hutauruk, Rufinus Hotmaulana. (2022). Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman. *Al-Manhaj: Jurnal Hukum dan Pranata Sosial Islam*,Vol.4,(No.2),pp.207-218. https://doi.org/10.37680/almanhaj.v4i2.1791

Cliza, Marta-Claudia., & Spataru-Negura, Laura-Cristina. (2018). The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? The rise of the data protection officer *Juridical Tribune*, Vol.8, Issue 2, pp.489-501.https://EconPapers.repec.org/RePEc:asr:journl:v:8:y:2018:i:2:p:489-501

Dhewa, Adithya Asmara., & Yossyafaat, Herkin. (2023). Aspek Hukum Perlindungan Konsumen Pada Transfer Data Pribadi

Oleh Korporasi dalam Hukum Positif Indonesia. *Lontar Merah,* Vol.6, (No.1), pp. 619-629. https://doi.org/10.31002/lm.v6i1.3807

Doly, D. (2021). Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru, *Negara Hukum*, Vol.12, (No.2), pp.223-244. https://dprexternal3.dpr.go.id/index.php/hukum/article/view/2357

Faizah, Azza Fitrahul., Rosadi, Sinta Dewi., Pratama, Garry Gumelar., & Dharmawan, Ananda Fersa. (2023). Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura. *Hakim: Jurnal Ilmu Hukum Dan Sosial*,Vol.1,(No.3),pp.1–27. https://journal.stekom.ac.id/index.php/Hakim/article/view/1222.

Gumzej, N. (2013). Selected aspects of proposed new EU general data protection legal framework and the Croatian perspective. *Juridical Tribune.* Vol.3, Issue 2, pp.178-201.https://EconPapers.repec.org/RePEc:asr:journl:v:3:y:2013:i:2:p:178-201

Juaningsih, Imas Novita., Hidayat, Rayhan Naufaldi., Aisyah, Kiki Nur., & Rusli, Dzakwan Nurirfan. (2021). Rekonsepsi Lembaga Pengawas Terkait Perlindungan Data Pribadi Oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi. *Salam: Jurnal Sosial dan Budaya Syar-i,* Vol.8, (No.1), pp.467–484. https://doi.org/10.15408/sjsbs.v8i2.19904

Latumahina, Rosalinda E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita,* Vol.3, (No.2), pp.14-25.https://id.scribd.com/document/358958953/Aspek-Hukum-Perlindungan-Data-Pribadi-Di-Dunia-Maya

Mahardika, Ahmad G. (2021). Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi dalam Sistem Ketatanegaraan Indonesia. *Jurnal Hukum UNISSULA*,Vol.37,(No.2),pp.101-118. https://doi.org/10.26532/jh.v37i2.16994

Matheus, Juan., & Gunadi, Ariawan. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *Justisi*, Vol.10, (No.1), pp.20-35. https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Pratama, Rizky., & Wulan, Evi Retno. (2023). Urgensitas Pembentukan Lembaga Penyelenggaraan Pelindungan Data Pribadi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, Vol.3, (No.2), pp.1828-1845. https://doi.org/10.53363/bureau.v3i2.291

Ramadani, R. (2020). Lembaga Negara Independen Di Indonesia Dalam Perspektif Konsep Independent Regulatory Agencies. *Jurnal Hukum Ius Quia Iustum,*

Vol.7,(No.1),pp.169-192. https://doi.org/10.20885/iustum.vol27.iss1.art9

Ramadhani, Syafira A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, Vol.3, (No.1), pp.73-84. https://doi.org/10.56370/jhlg.v3i1.173

Rizal, Muhammad S. (2019). Perbandingan Pelindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, Vol.10,(No.2),pp.218-227. https://doi.org/10.26905/idjch.v10i2.3349

Rumlus, Muhamad Hasan., & Hartadi, Hanif. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, Vol.11, (No.2), pp.285-299. https://doi.org/10.30641/ham.2020.11.285-299

Sahib, Nathania Salsabila Marikar., Idayanti, Soesi., & Rahayu, Kanti. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. *Pancasakti Law Journal*,Vol.1,(No.1),pp.62-74. https://doi.org/10.24905/plj.v1i1.8

Sandi, E. (2019). Pengawasan Otoritas Jasa Keuangan (OJK) terhadap Perbankan Sebagai Upaya Perlindungan Hukum Nasabah atas Penjualan Data Nasabah Bank. *Jurnal Idea Hukum*, Vol.5, (No.2), pp.1532-1543. https://doi.org/10.20884/1.jih.2019.5.2.125

Sangojoyo, Bram Freedrik., Kevin, Aurelius., & Sunlaydi, David Brilian. (2022) Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce di Indonesia. *Kosmik Hukum,* Vol. 22, (No.1), pp.27-39. https://doi.org/10.30595/kosmikhukum.v22i1.12154

Sautunnida, L. (2018). Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, Vol.20,(No.2),pp.369–384. https://doi.org/10.24815/kanun.v20i2.11159

Setiawan, Hezkiel Bram., & Najicha, Fatma Ulfatun. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, Vol.6,(No.1),pp.976-982. https://doi.org/10.31316/jk.v6i1.2657

Tsamara, N. (2021). Perbandingan Aturan Pelindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, Vol.3, (No.1),pp.53–85. https://doi.org/10.26740/jsh.v3n1.p53-84

Widjaja, Gunawan., & Cesarianti, Fransiska Milenia. (2024). 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. *Jurnal Riset*

*Ilmiah,*Vol.1,(No.4),pp.234–242. https://doi.org/10.62335/8qf44b59

Wolff, Josephine., & Atallah, Nicole. (2021). Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020. *Journal of Information Policy*, Vol.11, (No.1), pp.63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

Yuniarti, S. (2022). Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura. *Jurnal Becoss,* Vol.4,(No.2),pp.111-120. https://doi.org/10.21512/becossjournal.v4i2.8377

PROSIDING NASIONAL

Tumindak, Trengginas Teges., Ramadhiani, Alma Dwi., & Vivian. (2020). Transborder Data Flow Dalam Pelindungan Data Pribadi. In *Prosiding Konferensi Business Law 2020: Hukum Teknologi Informasi dan Komunikasi, Hukum Internasional dan Hukum Perdagangan* (pp.544-556). Jakarta: Business Law Publishing.

SKRIPSI

Lubis, Siti N. (2021). *Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara*. Universitas Hasanuddin.

BUKU

Ishaq. (2017). *Metode Penelitian Hukum dan Penulisan Skripsi Tesis serta Disertasi*. Bandung: Alfabeta.

SUMBER ONLINE

APJII. (2024). Survey Penetrasi Internet Indonesia 2024. Retrieved from https://survei.apjii.or.id/.

Banyu, R. (2023). Belajar dari gugatan terhadap Facebook di Eropa. Retrieved from https://Law.Ui.Ac.Id/Belajar-Dari-Gugatan-Terhadap-Facebook-Di-Eropa-Oleh-Rizky-Banyu-s-h-Ll-m/.

Iradat, D. (2024). Kominfo Sebut Lembaga Pengawas PDP Bakal Dibentuk Pertengahan 2024. Retrieved from https://www.cnnindonesia.com/teknologi/20240129132212-192-1055704/kominfo-sebut-lembaga-pengawas-pdp-bakal-dibentuk- Pertengahan-2024.

KlikLegal. (2021). Mau Mencontoh GDPR Milik Uni Eropa? Indonesia Perlu Perhatikan Hal-Hal Ini dalam Membuat Aturan Pelindungan Data Pribadi. Retrieved from https://appdi.or.id/mau-mencontoh-gdpr-milik-uni-eropa-indonesia-perlu-perhatikan-hal-hal-ini-dalam-membuat-aturan-pelindungan-data-pribadi/.

Sirie, Muhammad I. (2021). Tantangan Pengiriman Data Pribadi Lintas Negara. Retrieved from https://appdi.or.id/tantangan-pengiriman-data-pribadi-lintas-negara/.

Thea, A. (2022). Advokat Ini Ingatkan 3 Ketentuan Transfer Data Pribadi ke Luar Negeri. Retrieved from https://www.hukum online.com/Berita/a/Advokat-Ini-Ingatkan-3-Ketentuan-Transfer-Data-Pribadi-Ke-Luar-Negeri-Lt633baec525388/.

.