



Collaborative Governance sebagai Strategi Penguatan Pelindungan Data Pribadi di Indonesia: Analisis Peran Kementerian Koordinator Bidang Politik dan Keamanan

INFO PENULIS	INFO ARTIKEL
Shofiyah Aulia Universitas Muhammadiyah Jakarta auliashofi27@gmail.com Eva Permata Sari Hutagaol Kasubbag Tu Wamenko Polkam Khaerul Umam Noer Universitas Muhammadiyah Jakarta umam.noer@umj.ac.id	ISSN: 2808-1307 Vol. 6, No. 2, Agustus 2026 https://jurnal.ardenjaya.com/index.php/ajsh

© 2026 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi :

Aulia, S., Hutagaol, E. P. S., & Noer, K. U. (2026). Collaborative Governance sebagai Strategi Penguatan Pelindungan Data Pribadi di Indonesia: Analisis Peran Kementerian Koordinator Bidang Politik dan Keamanan. *Arus Jurnal Sosial dan Humaniora*, 6 (2),2225-2235.

Abstrak

Transformasi digital yang pesat di Indonesia, disertai dengan lonjakan pelanggaran data pribadi, telah menciptakan tantangan tata kelola dan keamanan siber yang tidak dapat diatasi oleh pemerintah saja. Studi ini bertujuan untuk menganalisis implementasi tata kelola kolaboratif sebagai strategi untuk memperkuat perlindungan data pribadi di Indonesia, dengan meneliti peran Kementerian Koordinator Bidang Politik dan Keamanan (Kemenko Polkam) sebagai koordinator lintas sektor. Dengan menggunakan pendekatan kualitatif deskriptif dengan metode tinjauan pustaka, studi ini meneliti dinamika kolaborasi berdasarkan kerangka teoritis model Tata Kelola Kolaboratif Ansell & Gash (2008) dan pendekatan pentahelix. Hasil penelitian menunjukkan bahwa implementasi tata kelola kolaboratif telah cukup berhasil pada tahap proses dan fondasi kelembagaan. Kementerian Koordinator Bidang Politik dan Keamanan telah secara efektif mengimplementasikan kepemimpinan fasilitatif sebagai titik fokus melalui pembentukan Desk Keamanan Siber dan Perlindungan Data, perumusan SOP untuk penanganan insiden, dan penyelarasan komunikasi antar aktor pemerintah, akademisi, bisnis, masyarakat sipil, dan media. Namun, efektivitas hasil akhirnya masih kurang optimal karena peraturan pelaksanaan Undang-Undang No. 27 Tahun 2022 (UU PDP). Ketidaklengkapan UU PDP, perbedaan pemahaman antar sektor, dan integrasi teknis yang terbatas, memerlukan komitmen dan penyempurnaan peraturan turunan yang berkelanjutan untuk menciptakan ekosistem digital nasional yang aman dan terintegrasi.

Kata Kunci: Tata Kelola Kolaboratif, Perlindungan Data Pribadi, Pelanggaran Data, UU PDP.

Abstract

The rapid digital transformation in Indonesia, accompanied by a surge in personal data breaches, has created governance and cybersecurity challenges that cannot be addressed by the government alone. This study aims to analyze the implementation of collaborative governance as a strategy to strengthen personal data protection in Indonesia, by examining the role of the Coordinating Ministry for Political and Security Affairs (Kemenko Polkam) as a cross-sector coordinator. Using a descriptive qualitative approach with a literature review method, this study examines the dynamics of collaboration based on the theoretical framework of the Ansell & Gash (2008) Collaborative Governance model and the pentahelix approach. The results indicate that the implementation of collaborative governance has been moderately successful in the process and institutional foundation stages. The Coordinating Ministry for Political and Security Affairs has effectively implemented facilitative leadership as a focal point through the establishment of a Cybersecurity and Data Protection Desk, the formulation of SOPs for incident handling, and the alignment of communication among government actors, academics, businesses, civil society, and the media. However, the effectiveness of the ultimate outcomes is still less than optimal due to the implementing regulations of Law No. The incompleteness of Law No. 27 of 2022 (PDP Law), varying understandings across sectors, and limited technical integration, require ongoing commitment and refinement of derivative regulations to create a secure and integrated national digital ecosystem

Key Words: Collaborative Governance, Personal Data Protection, Data Breach, PDP Law.

A. Pendahuluan

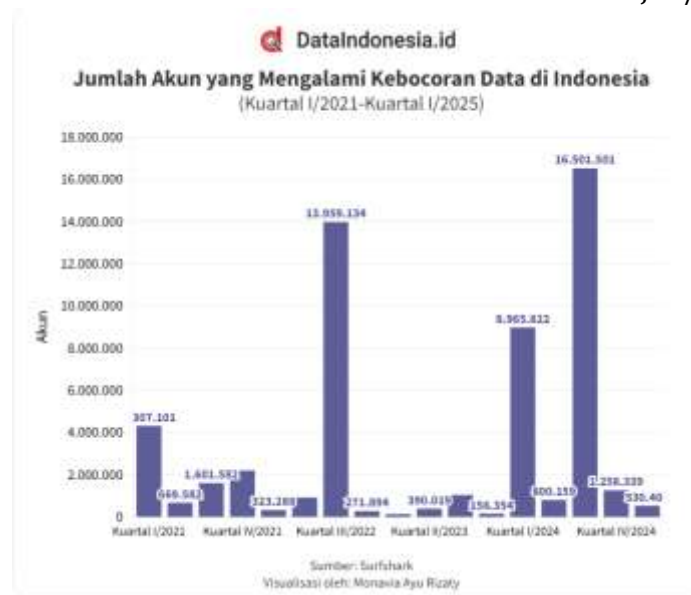
Transformasi digital telah memperluas penggunaan internet di hampir seluruh aspek kehidupan. Menurut survei APJII tahun 2025, pengguna internet Indonesia mencapai 229.428.417 dari total 284.430.900 jiwa (penetrasi 80,66%), naik dari 64,80% pada 2018 hingga 80,66% pada 2025 (inet.detik.com, 2025). Peningkatan akses ini membawa isu keamanan siber, ancaman, dan tantangan perlindungan data, sehingga persoalan data pribadi kini menjadi masalah tata kelola, keamanan, dan perlindungan hak warga di ruang digital.

Berbagai sektor termasuk layanan kesehatan digital, pertukaran data industri, pemerintahan digital, platform media sosial, dan aplikasi AIGC mengalami tantangan serupa terkait kebocoran dan penyalahgunaan data. Kesamaan ancaman ini menciptakan kondisi di mana para aktor yang berbeda menghadapi risiko bersama, saling bergantung satu sama lain, dan memerlukan kerangka aturan yang seragam. Oleh karena itu, fenomena tersebut menegaskan perlunya tata kelola kolaboratif (*collaborative governance*) yang mampu menyelaraskan peran, tanggung jawab, dan mekanisme koordinasi antar pemangku kepentingan untuk mengurangi kerentanan bersama dan memperkuat perlindungan data di ekosistem digital (Putri & Nusantara, 2024).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi dasar penting dalam pengaturan hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi atas pelanggaran data pribadi. Namun, dalam praktiknya, implementasi UU ini masih menghadapi hambatan berupa keterbatasan teknis, fragmentasi kebijakan, dan lemahnya koordinasi antar-lembaga. Karena itu, diperlukan pendekatan *collaborative governance* untuk memperkuat mitigasi dan penanganan pelindungan data pribadi di Indonesia, dengan Kementerian Koordinator Bidang Politik dan Keamanan Republik Indonesia berperan sebagai penghubung koordinasi lintas sektor (Küzeci, 2022).

Beberapa insiden kebocoran data di sektor pemerintahan, seperti dugaan kebocoran data BAIS TNI yang disebut bocor mencakup nama prajurit, pangkat, asal satuan, email, nomor telepon, hingga dokumen rahasia. Kemudian Inafis Polri mencakup gambar sidik jari, email, dan aplikasi *SpringBoot* yang telah dikonfigurasi, lalu diklaim dijual di dark web dengan harga tertentu (cnnindonesia.com, 2024).

Oleh karena itu, pendekatan *collaborative governance* relevan digunakan karena pelindungan data pribadi tidak dapat ditangani oleh pemerintah secara terpisah, melainkan memerlukan keterlibatan aktif aktor pemerintah, swasta, dan masyarakat sipil melalui partisipasi sejajar, dan pengambilan keputusan kolektif.



Sumber : DataIndonesia.id (2025)

Menurut laporan Surfshark, pada kuartal I 2025 terdapat 530.405 akun di Indonesia yang mengalami kebocoran data, turun 57,85% dari kuartal sebelumnya dan 94,08% dibanding kuartal I 2024. Meskipun demikian, tren kebocoran data domestik masih menunjukkan fluktuasi yang tinggi, dengan puncak tertinggi terjadi pada kuartal III 2024 sekitar 16,5 juta akun dan titik terendah pada kuartal I 2023 sebanyak 129.303 akun. Secara global, kuartal I 2025 mencatat 68,3 juta akun terdampak, sementara Amerika Serikat dan Rusia tetap menjadi negara dengan jumlah akun bocor terbesar. Dengan demikian, angka tersebut menunjukkan bahwa kebocoran data tidak hanya berdampak pada aspek teknis keamanan sistem, tetapi juga menimbulkan konsekuensi yang lebih luas terhadap perlindungan data pribadi dan kepercayaan publik terhadap tata kelola digital (DataIndonesia.id, 2025).

Berbagai penelitian terdahulu telah memberikan kontribusi terhadap pemahaman isu perlindungan data pribadi. (Lim & Oh, 2025) menyoroti perbandingan kebijakan perlindungan data di kawasan Asia-Pasifik dengan fokus pada adopsi norma global. Sementara (Sminorva & Travieso-Morales, 2024) membahas tantangan pengaturan data pribadi dalam tatanan hukum internasional yang semakin terhubung. Di Indonesia, kajian oleh (Kriswandaru et al., 2025) membahas landasan normatif UU PDP, sedangkan (Kharisma et al., 2024) mengkaji perlindungan data dalam konteks *e-commerce*. Meskipun kontribusi tersebut memberikan gambaran teoretis yang cukup kuat, namun sebagian besar studi masih bersifat deskriptif dan normatif, belum banyak yang menelaah secara empiris terkait koordinasi pemangku kepentingan dalam mitigasi dan penanganan kasus perlindungan data pribadi (Bisogno et al., 2024).

Meskipun penelitian-penelitian terdahulu telah memperkaya pemahaman mengenai perlindungan data pribadi dari aspek regulasi, harmonisasi kebijakan, maupun perlindungan hukum di sektor digital, fokus kajiannya masih didominasi oleh pendekatan normatif dan legalistik. Pendekatan tersebut memberikan kontribusi dalam menjelaskan substansi pengaturan perlindungan data pribadi, tetapi belum mampu menjelaskan bagaimana kebijakan tersebut diimplementasikan melalui mekanisme koordinasi antarpemangku kepentingan yang memiliki kewenangan dan kepentingan yang berbeda.

Di sisi lain, perlindungan data pribadi merupakan isu lintas sektor yang melibatkan berbagai aktor, seperti kementerian, lembaga pemerintah, penyelenggara sistem elektronik, aparat penegak hukum, serta masyarakat. Karakteristik tersebut menempatkan perlindungan data pribadi sebagai persoalan tata kelola yang tidak dapat diselesaikan hanya melalui pendekatan regulasi, melainkan membutuhkan proses kolaborasi yang mampu menyinergikan peran, sumber daya, dan kewenangan dari berbagai aktor yang terlibat. Namun demikian, belum pernah ada yang menganalisis perlindungan data pribadi melalui perspektif *Collaborative Governance*, khususnya yang menggunakan kerangka *Collaborative Governance* dari (Ansell & Gash, 2008) untuk menjelaskan dinamika kolaborasi antarpemangku kepentingan.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan menganalisis proses *Collaborative Governance* dalam penguatan perlindungan data pribadi di Indonesia dengan menelaah peran Kemenko Polkam sebagai koordinator lintas sektor. Pertanyaan penelitian yang diajukan adalah: Bagaimana *Collaborative Governance* menjadi strategi penguatan perlindungan data pribadi di Indonesia melalui peran koordinatif Kemenko Polkam?

B. Metodologi

Penelitian ini merupakan penelitian deskriptif dengan menggunakan pendekatan kualitatif dan metode pengumpulan data melalui studi literatur (*literatur review*) terhadap berbagai jurnal, buku, penelitian terdahulu, laporan pelaksanaan program, regulasi dan data sekunder lainnya terkait tema *collaborative governance*. Dengan studi literatur ini diharapkan peneliti dan pembaca mendapatkan gambaran awal dari tinjauan teori dan hasil penelitian serta pemantauan berbagai pihak yang relevan dengan kondisi yang ada untuk mengatasi permasalahan, sehingga dapat menjadi rujukan bagaimana peran aktor *Collaborative Governance* dalam penguatan perlindungan data pribadi.

Model Collaborative Governance yang digunakan dalam penelitian ini adalah Model (Ansell & Gash, 2008), menyampaikan bahwa terdapat empat tahapan dalam menjalankan proses kolaborasi yaitu: (1) Kondisi awal (*Starting Condition*), (2) Kepemimpinan fasilitatif (*Facilitative Leadership*), (3) Desain kelembagaan (*Institutional Design*), dan (4) Proses kolaborasi (*Collaborative Process*) terdiri dari : *Face to face dialogue* (dialog tatap muka), *Trust Building* (membangun kepercayaan), *Commitment to The Process* (komitmen terhadap proses), *Shared Understanding* (saling memahami), *Intermediate Outcome* (hasil akhir yang dicapai). Sementara itu konsep kolaborasi dalam model *penta helix* merupakan pengembangan dari model sebelumnya. Konsep ABCGM, yang mencakup Akademisi, Bisnis, Komunitas, Pemerintah, dan Media, mulai diidentifikasi sebagai model *penta helix* (Sri Afnitawati Rizky et al., 2024).

C. Hasil dan Pembahasan

Berdasarkan analisis terhadap seluruh dimensi *collaborative governance*, pelaksanaan tata kelola kolaboratif dalam strategi penguatan perlindungan data pribadi yang difasilitasi oleh Kementerian Koordinator Bidang Politik dan Keamanan (Kemenko Polkam) dapat dikategorikan berhasil pada tahap proses dan pembentukan fondasi kelembagaan (*moderately successful*). Keberhasilan ini ditunjukkan oleh kemampuan Kemenko Polkam dalam menjalankan kepemimpinan fasilitatif sebagai *focal point* dan orkestrator koordinasi nasional, yang berhasil memetakan serta menyelaraskan sumber daya para aktor *pentahelix* (pemerintah, akademisi, pelaku usaha, media, dan masyarakat sipil). Selain itu, kolaborasi ini telah membuahkan *intermediate outcomes* atau hasil antara yang konkret, seperti pembentukan Desk Keamanan Siber dan Pelindungan Data, pelembagaan saluran komunikasi bersama, penyiapan Standar Operasional Prosedur (SOP) penanganan insiden, serta lahirnya kesepahaman bersama (*shared understanding*) berbasis UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (Polkam.go.id, 2025).

Meski demikian, keberhasilan di tingkat proses dan fondasi awal ini belum sepenuhnya bertransformasi menjadi efektivitas hasil akhir (*ultimate outcomes*) yang optimal. Hal ini disebabkan oleh masih tingginya fluktuasi insiden kebocoran data di lapangan, aturan turunan UU PDP dan mekanisme integrasi teknis yang belum sepenuhnya lengkap, variasi pemahaman aturan antar-sektor, serta lembaga pengawas independen yang belum sepenuhnya mapan (Arief Budiono, 2026). Oleh karena itu, praktik *collaborative governance* ini dicapai melalui penguatan kapasitas negara dan konsolidasi lintas lembaga, namun keberhasilan substantifnya masih menuntut penyempurnaan aturan pelaksana, penguatan mekanisme pengawasan teknis, dan komitmen berkelanjutan dari seluruh pemangku kepentingan guna mewujudkan ketahanan siber serta kepercayaan publik yang berkelanjutan (Siber et al., 2018).

Pembahasan

Kondisi Awal (*Starting Condition*)

Dalam model kondisi awal (*starting condition*) memiliki 3 poin yaitu;

1. Ketidakseimbangan Sumber Daya

Pelindungan data pribadi tidak dapat dilaksanakan oleh satu instansi karena merupakan isu yang bersifat kompleks. Data pribadi masyarakat tersebar di berbagai instansi pemerintah (Komdigi, Kemenko Polkam, BSSN, dll), pemerintah daerah, lembaga keuangan, fasilitas kesehatan, perusahaan telekomunikasi, penyelenggara sistem elektronik, hingga platform digital. Kondisi tersebut menyebabkan setiap lembaga hanya memiliki kewenangan dan tanggung jawab pada bidang tertentu sehingga tidak ada satu institusi yang memiliki otoritas penuh untuk mengelola seluruh aspek perlindungan data pribadi. Selain itu, ancaman seperti kebocoran data dan serangan siber memerlukan penanganan yang didukung oleh koordinasi, pertukaran informasi, serta pemanfaatan sumber daya lintas lembaga (fh.untar.ac.id, 2025).

Ansell & Gash, (2008) menjelaskan bahwa pendekatan *Collaborative Governance* diterapkan ketika suatu persoalan melibatkan banyak aktor dengan kewenangan yang tersebar sehingga

memerlukan koordinasi, dialog, pembangunan kepercayaan, dan tujuan bersama. Setiap aktor memiliki peran yang saling melengkapi dalam mewujudkan perlindungan data pribadi yang efektif.

Kelompok Aktor	Contoh Aktor	Peran dalam Kolaborasi
Pemerintah	Kemenko Polkam	Sebagai koordinasi, sinkronisasi, dan pengendalian kebijakan perlindungan data pribadi agar pelaksanaannya terpadu di seluruh instansi
	Komdigi	Sebagai lembaga yang mengawasi, mengoordinasikan, dan menegakkan perlindungan data pribadi di ruang digital agar data warga tetap aman
	BSSN	Sebagai lembaga yang menjaga keamanan siber dan melindungi data pribadi dari ancaman, pencurian, serta penyalahgunaan di ruang digital
	Polri	Sebagai aparat penegak hukum yang menangani dan menindak kejahatan siber serta pelanggaran data pribadi
	Kemenkum	Sebagai pembinaan dan harmonisasi hukum agar perlindungan data pribadi sesuai dengan hak privasi dan ketentuan UU PDP
Akademisi	FH Unpad	Sebagai penyedia analisis hukum, penyusun naskah akademik
	FH UI	Mitra diskusi kebijakan, dan penguat literasi publik
	ATSI	Menjadi penghubung atau forum koordinasi antara industri, regulator, dan pihak lain terkait isu data pribadi.
Bisnis	MASTEL	Mengedukasi ekosistem digital agar lebih sadar keamanan data dan risiko penyalahgunaan data.
	APJII	Sebagai organisasi penyedia jasa internet yang mendukung regulasi, keamanan siber, edukasi masyarakat, dan pencegahan kebocoran data pribadi
Media Massa	Tempo	Sebagai media yang mengedukasi, mengawasi, dan mendorong perlindungan data pribadi, sekaligus menerapkan kebijakan privasi dalam kegiatan internalnya
	Kompas	Menjadi ruang publik untuk diskusi soal keamanan siber, privasi, dan tanggungjawab negara maupun masyarakat
Masyarakat (NGO)	ELSAM	Sebagai lembaga advokasi yang mengawal kebijakan, mendorong pengawasan independen, dan memperjuangkan perlindungan data pribadi sebagai bagian dari hak asasi manusia
	SafeNet	Sebagai organisasi masyarakat sipil yang mengawal hak privasi, mendorong pengawasan UU PDP, dan memperkuat perlindungan data pribadi warga

Sumber : Diolah Penulis dari Berbagai Sumber

Perbedaan sumber daya ini menunjukkan bahwa setiap aktor tidak berada pada posisi yang sama dalam kolaborasi, sehingga diperlukan mekanisme yang adil agar keunggulan satu pihak tidak mendominasi pihak lain. Oleh karena itu, pemetaan sumber daya aktor menjadi penting untuk memastikan bahwa kolaborasi *pentahelix* dapat berjalan secara seimbang, saling melengkapi, dan efektif dalam memperkuat perlindungan data pribadi.

1.1 Insentif untuk Berpartisipasi

Aktor	Insentif/Manfaat Partisipasi	Penjelasan
Pemerintah	Penguatan tata kelola dan kepercayaan publik	Memperkuat perlindungan warga, menciptakan tata kelola data yang lebih akuntabel, memperluas sosialisasi kebijakan, mempercepat identifikasi risiko kebocoran data, meningkatkan efektivitas pengawasan, serta membangun kepercayaan dan legitimasi pemerintah dalam penyelenggaraan layanan digital.
Akademisi	Pengembangan ilmu pengetahuan dan penelitian terapan	Memperoleh peluang melakukan penelitian yang relevan dengan kebutuhan masyarakat, mengembangkan konsep dan teori, menghasilkan rekomendasi berbasis bukti, memperoleh akses terhadap data lapangan dan kasus nyata, serta memperkaya proses pembelajaran dan pengembangan keilmuan.
Pelaku Usaha	Kepastin hukum, dan keberlanjutan bisnis	Memperoleh kepastian hukum, meningkatkan kepercayaan konsumen, memperkuat citra perusahaan sebagai organisasi yang bertanggung jawab, mengurangi risiko sanksi dan kebocoran data, serta mendukung keberlanjutan usaha melalui pengelolaan data yang aman.
Komunitas/Masyarakat	Perlindungan hak dan peningkatan literasi digital	Meningkatkan kesadaran mengenai pentingnya perlindungan data pribadi, memahami hak sebagai subjek data, memperoleh edukasi terkait keamanan data, mengenali risiko kebocoran data, serta berperan aktif dalam menjaga ekosistem digital yang sehat.
Media	Penguatan fungsi edukasi dan kontrol sosial	Menjalankan fungsi penyebaran informasi, edukasi publik, dan pengawasan terhadap pengelolaan data oleh pemerintah maupun sektor swasta.

Sumber : Diolah Penulis dari Berbagai Sumber

Sejarah Konflik atau Kerjasama

Kondisi pada tahap ketakutan akan terjadinya konflik dapat berupa perbedaan pendapat antara pemangku kepentingan, swasta, dan pihak yang ikut berpartisipasi. Pada dasarnya semua pihak yang ikut berkolaborasi memiliki visi bersama yang ingin dicapai. Namun Ansel dan Gash mencatat bahwa ketika para pemangku kepentingan saling ketergantungan tingkat konflik yang tinggi dapat memberikan keuntungan yang besar untuk collaborative governance (Ansel dan Gash, 2008).

Konflik yang tinggi tidak selalu menjadi penghalang untuk berkolaborasi dan dalam mencapai tujuan tidak akan berhasil tanpa terlibat dalam proses kolaborasi walaupun ada kepentingan dari stakeholders lain yang bertentangan. Ketidak selarasan pemikiran yang terjadi antara stakeholders justru akan menghasilkan kebijakan baru dalam suatu permasalahan yang bisa memecahkan konflik yang tidak dapat terselesaikan sebelumnya (unair.ac.id, 2024).

Perhatian terhadap perlindungan data pribadi muncul seiring meningkatnya penggunaan data digital dan bertambahnya risiko penyalahgunaan, sehingga pendekatan yang hanya bertumpu pada satu pihak dinilai tidak memadai. Dalam konteks Indonesia, kerangka awal perlindungan data

cenderung bersifat top-down melalui regulasi pemerintah, termasuk peran Kemenkominfo dalam pengaturan awal sistem elektronik dan perlindungan data pribadi. Proses pembahasan RUU PDP juga berlangsung panjang sejak lama dan melalui tahapan harmonisasi antarlembaga sebelum akhirnya disahkan menjadi UU PDP, yang menunjukkan kompleksitas penyusunan kebijakan ini (indonesiabaik.id, 2023)

Kerja sama mulai menguat lewat forum lintas pemangku kepentingan dan model *multistakeholder*, misalnya kolaborasi lintas sektor dalam tata kelola data digital dan internet *governance*. Ini menunjukkan bahwa isu perlindungan data pribadi tidak bisa diselesaikan oleh pemerintah sendiri, melainkan perlu peran pemerintah, sektor usaha, akademisi, masyarakat sipil, dan media (unesdoc., 2023).

Konflik terutama muncul karena perbedaan kepentingan dan pembagian kewenangan. Pemerintah cenderung menekankan pengawasan dan kepatuhan, sektor usaha menyoroti kepastian hukum dan beban implementasi, sementara masyarakat sipil lebih menekankan hak privasi dan pengawasan yang kuat. Selain itu, konflik norma juga bisa muncul antara perlindungan data dan kebebasan pers atau kebutuhan berbagi data antarinstansi (Novianti & Tengah, 2025).

Konflik tidak selalu dianggap sebagai penghalang utama, melainkan sebagai bagian dari proses yang perlu dikelola melalui saling percaya, dan forum koordinasi. Oleh karena itu, perjalanan kerja sama dalam perlindungan data pribadi di Indonesia dapat dipahami sebagai proses bertahap, yaitu bergerak dari pengaturan yang lebih terpusat menuju kolaborasi lintas sektor yang lebih terbuka, meskipun masih ada tantangan dalam integrasi, penyamaan standar, dan konsistensi pengawasan (komdigi.go.id, 2024).

2. Kepemimpinan Fasilitatif (*Facilitative Leadership*)

Kepemimpinan fasilitatif merupakan unsur kunci dalam *Collaborative Governance*. Dalam buku harian mereka, (Ansell & Gash, 2008) menulis, “Kepemimpinan sangat penting untuk menetapkan dan memelihara aturan-aturan dasar yang jelas, membangun kepercayaan, mendorong dialog, dan mengeksplorasi kepentingan bersama.” Pemanfaatan kepemimpinan bertujuan untuk memberdayakan dan menggerakkan pemangku kepentingan agar dapat meningkatkan proses kolaboratif. Oleh karena itu, kepemimpinan yang efektif dan bertanggung jawab akan menghasilkan proses kolaborasi yang sukses.

Salah satu aspek penting dalam kepemimpinan yang memfasilitasi adalah kemampuan mengidentifikasi titik fokus atau *focal point* dalam kolaborasi. Pada model *pentahelix*, aktor yang terlibat meliputi pemerintah, akademisi, pelaku usaha, komunitas, dan media. Meskipun seluruh aktor memiliki kontribusi masing-masing, diperlukan satu atau lebih titik fokus yang berfungsi sebagai simpul koordinasi agar proses kolaborasi tidak berjalan parsial dan terfragmentasi. Dalam isu perlindungan data pribadi, titik fokus tersebut dapat berada pada institusi pemerintah sebagai pemegang mandat regulatif, atau pada lembaga koordinator yang memiliki kapasitas menjembatani kebutuhan teknis, kebijakan, dan edukasi publik (Magda Faradiba, 2025).

Selain menentukan titik fokus, kepemimpinan fasilitatif juga menuntut pengelolaan proses dialog secara sistematis. Dialog dalam kolaborasi *pentahelix* tidak boleh dipahami sebagai percakapan informal semata, melainkan sebagai mekanisme deliberatif untuk menyamakan persepsi, menyusun agenda bersama, dan menyelesaikan perbedaan kepentingan. Proses dialog yang baik harus dibangun di atas prinsip keterbukaan, kesetaraan partisipasi, dan orientasi pada pemecahan masalah. Dengan demikian, setiap aktor dapat menyampaikan perspektifnya sesuai peran dan kapasitas masing-masing tanpa kehilangan arah kolaborasi.

Dalam praktiknya, dialog yang dikelola secara efektif akan membantu memetakan pembagian peran antarpemangku kepentingan. Pemerintah berperan dalam penyusunan regulasi dan pengawasan, akademisi berkontribusi melalui kajian ilmiah dan rekomendasi kebijakan, pelaku usaha menyediakan dukungan implementatif dan teknologi, komunitas mendorong partisipasi publik serta literasi, sedangkan media berfungsi sebagai saluran diseminasi informasi dan kontrol sosial. Kepemimpinan yang memfasilitasi diperlukan untuk memastikan bahwa pembagian peran tersebut tidak tumpang tindih dan tetap selaras dengan tujuan perlindungan data pribadi (Magda Faradiba, 2025).

Dengan demikian, keberhasilan kolaborasi perlindungan data pribadi model *pentahelix* sangat bergantung pada kemampuan pemimpin dalam menetapkan *focal point* yang jelas serta mengelola dialog lintas aktor secara konstruktif. Kepemimpinan fasilitatif memungkinkan terciptanya koordinasi yang lebih efektif, pengambilan keputusan yang lebih partisipatif, dan implementasi kebijakan yang lebih konsisten. Dalam konteks tata kelola perlindungan data pribadi, pendekatan ini menjadi penting karena isu yang dihadapi bersifat kompleks, lintas sektor, dan memerlukan sinergi multipihak (Multidisiplin & Sosial, 2026).

3. Desain kelembagaan (*Institutional Design*)

Desain Kelembagaan (*institutional design*) dalam perlindungan data pribadi menurut Ansell & Gash, (2008) merupakan kerangka pengaturan yang menentukan bagaimana aktor-aktor yang terlibat berinteraksi, mengambil keputusan, dan menjalankan fungsi pengawasan secara efektif. Dalam konteks tata kelola data pribadi, desain institusional tidak cukup hanya menempatkan lembaga atau aktor tertentu sebagai pengelola utama, tetapi juga harus memastikan adanya mekanisme kerja yang partisipatif, forum kolaborasi yang jelas, serta transparansi yang memadai. Ketiga unsur tersebut penting untuk membangun legitimasi, akuntabilitas, dan efektivitas perlindungan data pribadi.

1. Partisipasi

bahwa perlindungan data pribadi harus melibatkan berbagai pemangku kepentingan secara bermakna. Partisipasi tidak hanya berarti kehadiran formal, melainkan juga keterlibatan aktif dalam perumusan kebijakan, penyusunan standar, dan evaluasi pelaksanaan. Dalam kerangka perlindungan data pribadi, partisipasi subjek data, pemerintah, penyelenggara sistem elektronik, akademisi, masyarakat sipil, dan sektor usaha menjadi penting agar kebijakan yang dihasilkan tidak bersifat sepihak. Prinsip partisipasi juga sejalan dengan hak individu untuk mengetahui, mengakses, dan melakukan koreksi atas data pribadinya (bphn.go.id, 2011).

2. Forum kolaborasi

Ruang kelembagaan yang memungkinkan para aktor berdialog, bernegosiasi, dan menyelaraskan kepentingan. Forum ini diperlukan karena isu perlindungan data pribadi bersifat lintas sektor dan tidak dapat diselesaikan hanya melalui pendekatan sektoral. Dalam praktiknya, forum kolaborasi dapat berbentuk dewan, komite, sekretariat bersama, kelompok kerja lintas institusi, atau mekanisme koordinasi reguler yang mempertemukan regulator, pelaku industri, dan pemangku kepentingan lain. Keberadaan forum kolaborasi yang terstruktur akan memudahkan pembagian peran, mencegah tumpang tindih kewenangan, serta memperkuat koordinasi dalam merespons pelanggaran maupun pengembangan kebijakan (peraturan.bpk.go.id, 2022).

3. Transparansi

Transparansi menuntut adanya kejelasan mengenai kewenangan lembaga, prosedur pengambilan keputusan, dasar pemrosesan data, serta mekanisme pengaduan dan pengawasan. Dalam perlindungan data pribadi, transparansi juga mencakup kewajiban untuk memberikan informasi yang mudah dipahami kepada masyarakat mengenai tujuan pengumpulan data, pihak yang dapat mengakses data, jangka waktu penyimpanan, dan hak-hak subjek data. Tanpa transparansi, partisipasi hanya menjadi formalitas dan forum kolaborasi berisiko kehilangan akuntabilitasnya (Marsya Iffah et al., 2025).

Ketiga aspek tersebut saling berkaitan dan tidak dapat dipisahkan. Partisipasi yang luas membutuhkan forum kolaborasi yang inklusif, sedangkan forum kolaborasi hanya akan efektif apabila dijalankan secara transparan. Dalam konteks perlindungan data pribadi, desain institusional yang baik harus mampu menciptakan keseimbangan antara efektivitas pengambilan keputusan dan keterbukaan terhadap pengawasan publik. Dengan demikian, institusi yang dibangun tidak hanya berfungsi sebagai pengatur, tetapi juga sebagai penghubung kepentingan yang menjamin pelaksanaan perlindungan data secara konsisten dan akuntabel (Marsya Iffah et al., 2025).

Secara keseluruhan, desain institusional dalam perlindungan data pribadi harus dirancang sebagai sistem yang partisipatif, kolaboratif, dan transparan. Pendekatan ini penting agar kebijakan tidak berhenti pada tataran normatif, melainkan benar-benar dapat diterapkan dalam praktik. Dengan adanya partisipasi yang bermakna, forum kolaborasi yang terstruktur, dan transparansi yang kuat, perlindungan data pribadi dapat berjalan lebih efektif sekaligus memperkuat kepercayaan masyarakat terhadap tata kelola data di Indonesia (Lailatul Badriah, 2024).

4. Proses Kolaborasi (*Collaborative Process*)

a. *Face to face dialogue* (Dialog Tatap Muka)

Ansell & Gash, (2008) menyatakan bahwa langkah awal dalam tata kelola kolaboratif melibatkan interaksi tatap muka antara pemangku kepentingan yang berbeda. Tahap ini dianggap sebagai elemen paling krusial karena membantu membangun kepercayaan, saling menghormati, pemahaman, dan komitmen terhadap seluruh proses. Tahapan kolaborasi meliputi tahap pranegosiasi, tahap negosiasi dan pelaksanaan rencana.

Dalam mitigasi dan penanganan perlindungan data pribadi, Kemenko Polkam memfasilitasi pertemuan tatap muka antarkementerian, lembaga teknis, aparat penegak hukum, dan sektor terkait untuk menyamakan pembacaan risiko, mandat, dan jalur eskalasi. Indonesia menekankan bahwa sinergi lembaga negara adalah kunci perlindungan data dan ketahanan siber, sedangkan koordinasi yang berjalan baik memperkuat perlindungan terhadap ancaman siber. Bukti lintas

kasus juga menunjukkan bahwa koordinasi biasanya dimulai ketika para aktor menyadari masalah bersama yang tidak dapat diselesaikan satu lembaga saja.

Dialog tatap muka tidak cukup bila hanya seremonial. Bukti menunjukkan bahwa koordinasi melemah saat hubungan interpersonal lemah, tidak ada liaison sebelumnya, struktur pelaporan terlalu rumit, atau sistem informasi terfragmentasi. Tata kelola kolaboratif yang efektif hanya dapat dicapai dengan mengadakan pertemuan tatap muka. Rekomendasi ini didasarkan pada teori Meyer dan O'Toole Jr. (2002) yang disajikan dalam penelitian oleh (Idris, 2022). Menurut teori ini, kesuksesan program ditekankan pada proses kolaboratif antar organisasi yang memerlukan kerjasama.

b. Trust Building (Membangun Kepercayaan)

Kepercayaan memiliki peran krusial dalam kerjasama, karena tidak hanya melibatkan proses tawar menawar, tetapi juga membangun kepercayaan antara setiap pemangku kepentingan terlibat (Ansell & Gash, 2007). Pada fase awal kolaborasi, pertemuan bilateral, kehadiran fisik, dan komunikasi informal membantu mengurangi salah paham dan memperkuat trust di banyak level organisasi (Groot Jans, 2022). Dalam peran Kemenko Polkam, membangun kepercayaan berarti mengoordinasikan kementerian, lembaga, dan sektor privat agar mitigasi serta penanganan pelanggaran data tidak berjalan parsial. Kemenko Polkam karena itu paling tepat berperan sebagai orkestrator koordinasi yang menyatukan respons insiden, komunikasi antarlembaga, dan agenda peningkatan kesadaran publik.

c. Commitment to The Process (Komitmen Terhadap Proses)

Keberhasilan suatu kegiatan tidak dapat dicapai tanpa adanya komitmen yang tinggi dari pelakunya terhadap proses pelaksanaan. Oleh karena itu, hal ini menjadi masalah ketika kurangnya keterlibatan pemangku kepentingan (Ansell & Gash, 2008). Selain itu, keterlibatan sebenarnya adalah keyakinan bahwa tata kelola kolaboratif menguntungkan setiap pihak dan kepentingan publik.

Dalam konteks perlindungan data pribadi, komitmen terhadap proses menuntut adanya isu yang sama sebagai dasar penyatuan kepentingan. Isu yang sama berfungsi sebagai titik temu yang memungkinkan berbagai sektor bergerak dalam arah yang serupa. Misalnya, perlindungan hak subjek data, pencegahan penyalahgunaan data, peningkatan kepatuhan, dan penguatan keamanan pemrosesan data dapat menjadi agenda bersama yang diakui oleh pemerintah, pelaku usaha, akademisi, masyarakat sipil, dan media. Kesamaan isu ini penting karena kolaborasi lintas sektor hanya dapat berkembang jika para pihak memiliki fokus yang dipahami bersama sejak awal.

Namun, kesamaan isu saja belum cukup apabila tidak disertai pemahaman yang sama antar sektor mengenai makna, urgensi, dan implikasi dari isu tersebut. Setiap sektor dapat membawa perspektif yang berbeda: pemerintah cenderung memandang perlindungan data pribadi sebagai instrumen regulatif dan pengawasan, sektor usaha melihatnya sebagai kewajiban kepatuhan dan tata kelola risiko, sedangkan masyarakat sipil menekankan aspek hak, privasi, dan perlindungan warga. Perbedaan perspektif ini merupakan hal yang wajar dalam kolaborasi multiaktor, tetapi harus dikelola melalui proses dialog yang memungkinkan lahirnya definisi bersama atas masalah dan solusi yang hendak dicapai.

Pemahaman yang sama menjadi penting karena kolaborasi tidak hanya membutuhkan kesepakatan tujuan, tetapi juga keselarasan dalam terminologi, pembagian tugas, dan mekanisme kerja. Dalam praktiknya, bila tiap sektor menafsirkan isu perlindungan data pribadi secara berbeda, maka koordinasi dapat terganggu, prioritas kebijakan menjadi tidak seragam, dan implementasi kebijakan kehilangan arah. Oleh karena itu, proses kolaboratif harus mencakup tahap *discovery*, penyamaan istilah, perumusan tujuan bersama, dan negosiasi peran agar semua pihak memiliki referensi yang sama dalam bertindak.

Dengan demikian, *commitment to the process* dalam kolaborasi perlindungan data pribadi mensyaratkan adanya isu bersama dan pemahaman bersama antar sektor. Kedua unsur tersebut menjadi fondasi agar kolaborasi tidak berjalan secara fragmentaris, melainkan terarah, sinkron, dan berorientasi pada hasil. Jika para aktor memiliki fokus isu yang sama dan kerangka pemahaman yang serupa, maka peluang terbentuknya kerja sama yang efektif, adaptif, dan berkelanjutan akan semakin besar.

d. Shared Understanding (Saling Memahami)

Ansell & Gash, (2008) menyatakan bahwa pemangku kepentingan perlu memiliki pemahaman yang seragam mengenai kolaborasi, termasuk visi, misi, tujuan yang terdefinisi dengan jelas, dan penyesuaian terhadap inti permasalahan. Bustomi et al., (2022) menambahkan bahwa pada tahap tertentu dalam proses kolaborasi, penting bagi pihak-pihak terlibat untuk mengembangkan pemahaman bersama tentang pencapaian yang dapat diraih secara bersama-sama.

Komdigi dan BSSN telah menunjukkan sinergi dalam penguatan keamanan siber dan perlindungan data pribadi, sementara peran pemangku kepentingan lain seperti Polri dan ELSAM penting dalam memperkuat koordinasi, pengawasan, dan advokasi kebijakan. Kolaborasi

antarpihak ini pada dasarnya diarahkan untuk memperkuat tata kelola perlindungan data pribadi dan menekan risiko kebocoran data (komdigi.go.id, 2024).

Dalam berbagai dimensi aktor juga sudah memahami bahwa perlindungan data membutuhkan kolaborasi lintas sektor, bukan pendekatan satu lembaga saja. Namun, pemahaman itu belum seragam penuh. Kesadaran dan pemahaman atas hukum perlindungan data masih bervariasi, bahkan ketika para aktor sudah mengenal regulasi yang sama. Definisi privasi, batas penggunaan data, dan cara menerapkan aturan juga masih sering kabur atau belum diterima secara sama oleh semua pihak (Lindra Darnela et al., 2025).

e. *Intermediate Outcome* (Hasil Akhir yang Dicapai)

Menurut Ansell dan Gash (2008), *Intermediate Outcomes* atau hasil antara merupakan indikator krusial yang menandai berjalannya proses kolaborasi sebelum manfaat jangka panjang terwujud secara penuh. Pada konteks strategi penguatan perlindungan data pribadi di Indonesia, hasil antara yang realistis bukanlah terhentinya seluruh kasus kebocoran data secara mendadak, melainkan terbangunnya tata kelola lintas sektor yang lebih operasional, terstruktur, dan sinkron. Berdasarkan analisis peran Kementerian Koordinator Bidang Politik dan Keamanan (Kemendagri) sebagai fasilitator dan orkestrator koordinasi nasional, capaian hasil antara ini dapat diidentifikasi melalui beberapa bentuk konkret. Pertama, hadirnya program strategis seperti pembentukan *Desk Keamanan Siber dan Pelindungan Data* oleh Kemendagri yang berfungsi menyelaraskan fungsi-fungsi antar Kementerian/Lembaga serta merumuskan Rencana Aksi Nasional yang terintegrasi. Langkah ini mengikis ego sektoral dengan menyatukan kementerian dan lembaga teknis, seperti Komdigi, BSSN, Polri, dan Kemenkum, dalam satu koridor kerja yang sama (Kemendagri.go.id, 2025).

Selain penyelarasan program, hasil antara yang signifikan ditunjukkan oleh perumusan Standar Operasional Prosedur (SOP) penanganan pelanggaran data dan pelembagaan saluran komunikasi bersama antar kementerian (Prosedur, 2024). Adanya SOP dan mekanisme komunikasi terpadu ini memberikan kejelasan jalur eskalasi, tata cara pelaporan, serta pembagian kewenangan antara lembaga pengawas dan aparat penegak hukum ketika insiden kebocoran data terjadi. Di samping itu, landasan hukum dan kelembagaan yang semakin kuat setelah pengesahan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) turut mendorong penyamaan persepsi di antara para aktor *pentahelix*. Kerja sama ini tidak hanya melibatkan aktor pemerintah, tetapi juga merangkul pelaku usaha (seperti APJII, ATSI, MASTEL), akademisi, media massa (seperti Kompas dan Tempo), serta organisasi masyarakat sipil (seperti ELSAM dan SAFEnet) untuk meningkatkan kapasitas pencegahan dan literasi publik mengenai perlindungan data (peraturan.go.id, 2022).

Meskipun capaian hasil ini berhasil memperkuat kapasitas negara dalam merespons insiden, berbagai studi mencatat bahwa efektivitasnya masih terbatas oleh aturan pelaksana yang belum lengkap, integrasi teknis yang terbatas, serta pengawasan independen yang belum sepenuhnya mapan (Kaharuddin et al., 2026). Oleh karena itu, hasil antara yang tercapai sejauh ini masih menuntut evaluasi dan penyempurnaan berkelanjutan. Demikian, pencapaian *intermediate outcomes* tersebut menjadi fondasi utama yang akan menjembatani kolaborasi menuju hasil yang diharapkan, yaitu meningkatnya kepercayaan publik terhadap tata kelola digital, terciptanya percepatan respons atas ancaman siber, terkikisnya kesenjangan keahlian antara sektor publik dan swasta, serta terwujudnya ekosistem digital nasional yang aman dan terintegrasi.

D. Kesimpulan

Penelitian ini menunjukkan bahwa pendekatan *collaborative governance* menjadi salah satu strategi yang tepat dalam memperkuat perlindungan data pribadi di Indonesia. Karakteristik permasalahan perlindungan data yang melibatkan banyak pihak dengan kewenangan dan kepentingan yang berbeda menjadikan kolaborasi sebagai kebutuhan dalam penyelenggaraan tata kelola. Berdasarkan analisis menggunakan model *Collaborative Governance* Ansell dan Gash, keterlibatan pemerintah, pelaku usaha, akademisi, masyarakat sipil, dan media mampu menciptakan sinergi yang mendukung implementasi perlindungan data pribadi. Dalam hal ini, Kementerian Koordinator Bidang Politik dan Keamanan berperan sebagai koordinator yang menghubungkan berbagai aktor sehingga proses koordinasi dan penyelarasan kebijakan dapat berjalan lebih terarah.

Temuan penelitian memperlihatkan bahwa proses kolaborasi telah berkembang melalui terbentuknya kepemimpinan yang fasilitatif, forum koordinasi lintas sektor, serta adanya dialog, kepercayaan, komitmen, dan pemahaman bersama di antara para pemangku kepentingan. Kondisi tersebut menghasilkan beberapa capaian awal yang penting, seperti pembentukan *Desk Keamanan Siber dan Pelindungan Data*, penyusunan standar operasional prosedur penanganan insiden, serta penguatan mekanisme komunikasi antar lembaga. Capaian tersebut menunjukkan bahwa tata

kelola perlindungan data pribadi di Indonesia telah memiliki fondasi kelembagaan yang semakin baik sebagai dasar untuk meningkatkan efektivitas koordinasi lintas sektor.

Meskipun demikian, penguatan perlindungan data pribadi masih menghadapi berbagai tantangan yang perlu mendapat perhatian. Belum optimalnya aturan pelaksana, keterbatasan integrasi teknis antarlembaga, serta mekanisme pengawasan yang masih perlu diperkuat menunjukkan bahwa kolaborasi yang telah dibangun belum sepenuhnya menghasilkan dampak yang optimal terhadap penurunan kasus kebocoran data. Oleh karena itu, diperlukan komitmen yang berkelanjutan dari seluruh pemangku kepentingan untuk memperkuat implementasi regulasi, meningkatkan koordinasi lintas sektor, dan mengembangkan sistem pengawasan yang lebih efektif sehingga tujuan perlindungan data pribadi serta peningkatan kepercayaan masyarakat terhadap ekosistem digital nasional dapat tercapai secara lebih optimal.

E. Referensi

- Awareness, P., Darnela, L., Rusdiana, E., Islam, U., Sunan, N., Yogyakarta, K., & Madura, U. T. (2025). *Supremasi Hukum : Jurnal Kajian Ilmu Hukum*. 14(1), 1–28. <https://doi.org/10.14421/2gg2rp29>
- Bumiaji, D., & Wisata, K. (2021). *Jurnal Ilmiah Administrasi Publik (JIAP) Collaborative Governance dalam Tata Kelola Pariwisata-Desa (Studi Pariwisata-*. 7(1), 20–29.
- Hanaya, E. (2023). Perlindungan Data Pribadi di Era Digital Dalam Perspektif Perbandingan Hukum. *Jurnal Bevinding*, 1(9), 11–22.
- Hukum, F., & Surakarta, U. M. (2026). *TENTANG PERLINDUNGAN DATA PRIBADI DALAM MENJAMIN KEAMANAN DATA PRIBADI DI ERA DIGITAL*. 3(3), 951–964.
- Ilmiah, J., & Pendidikan, W. (2026). *No Title*. 12(June), 26–34.
- Jurnal, E., Hukum, I., Iffah, M., Raib, E., Rosadi, S. D., & Cahyadi, A. (2025). *Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi Fakultas Hukum, Universitas Padjadjaran, Indonesia dunia, termasuk Indonesia. Menurut data yang diperoleh dari hasil survei yang dilakukan oleh Gambar 1. Jumlah Pengguna Internet Tahun 2023 kehidupan sehari-hari masyarakat di Indonesia. Hal ini didukung oleh data yang diperoleh bahwa persentase penetrasi internet di Indonesia pada tahun 2024 telah mencapai 79, 5 % dari 3.*
- Küzeci, E. (2022). Personal Data Protection Law. *Introduction to Turkish Business Law*, 016999, 457–483.
- Multidisiplin, J., & Sosial, I. (2026). *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*. 11(10).
- Novarianti, W. D., & Tengah, J. (2025). *Kerahasiaan Bank vs Hak Atas Informasi : Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi*. 2(1), 103–114.
- Pengantar, K. (2011). *Naskah akademik rru perlindungan data pribadi*.
- Persampahan, P., Kabupaten, D., Rizky, S. A., & Saputra, A. P. (2024). *Model Collaborative Governance*. 24(1), 12–29.
- Prosedur, S. O. (2024). *Standar operasional prosedur*. 1–4.
- Publicuho, J., Faradiba, M., & Agung, M. (2025). *STRENGTHENING GOVERNANCE THROUGH PENTAHILIX COLLABORATION : A QUALITATIVE STUDY IN THE ERA OF DIGITAL*. 8(3), 1619–1626.
- Putri, A. K., & Nusantara, U. M. (2024). *Peran Security Analyst...*, Azalea Keisha Putri, Universitas Multimedia Nusantara. 2023–2026.
- Selatan, K. (2024). *Akuntabilitas dalam Kebijakan Perlindungan Data Pribadi di Indonesia*. 8, 89–102.
- Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, 6(1), 976–982.
- Siber, B., Negara, S., Insiden, P. P., Siber, B., & Sandi, D. A. N. (n.d.). *Panduan penanganan insiden serangan sql injection*.
- Tahun, U. U. N. O., Saly, J. N., Artamevia, H., Kheista, K., Juni, B., Gulo, S., Rhemrev, E. A., & Christie, M. (2023). *ANALISIS PERLINDUNGAN DATA PRIBADI TERKAIT*. 1(3), 145–153.