



Perlindungan Data Pribadi Dalam Era Big Data : Implikasi Hukum Di Indonesia

Rengga Kusuma Putra*¹, Maulana Fahmi Idris², Greget Widhiati³

¹Universitas Sains dan Teknologi Komputer Semarang, renggakusuma@stekom.ac.id

²Universitas Sains dan Teknologi Komputer Semarang, maulanafahmi@stekom.ac.id

³Universitas Sains dan Teknologi Komputer Semarang, greget.stekom@gmail.com

Abstract

This study examines the challenges and effectiveness of the Personal Data Protection Law (UU PDP) in Indonesia amidst the rapid expansion of Big Data. As digital data collection and processing become increasingly integral across sectors, this study identifies gaps in policy implementation, particularly among small and medium enterprises (SMEs), which often lack resources for comprehensive data protection. Through interviews and document analysis, findings indicate that while the UU PDP establishes a necessary legal framework, its implementation faces obstacles, including limited adoption of encryption and anonymization technologies and low public awareness of data privacy risks. These challenges highlight the need for enhanced governmental support, technical guidelines, and public education to improve data security practices. This study contributes to ongoing policy discussions by offering practical recommendations to strengthen data protection in Indonesia and foster a safer digital environment for individuals.

Keywords: Personal Data Protection Law, Big Data, public awareness, data protection policy

I. INTRODUCTION

Perkembangan pesat teknologi informasi dan komunikasi, terutama dalam era Big Data, telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Big Data merujuk pada volume data yang sangat besar, beragam, dan cepat yang dihasilkan oleh aktivitas digital sehari-hari (Bibri et al. 2023). Data ini dihasilkan tidak hanya oleh individu, tetapi juga oleh organisasi, perusahaan, dan pemerintah melalui berbagai interaksi digital, termasuk media sosial, e-commerce, layanan kesehatan, dan sensor perangkat Internet of Things (IoT) (Sunhare, Chowdhary, and Chattopadhyay 2022). Menurut laporan terbaru, diperkirakan bahwa jumlah data yang dihasilkan secara global meningkat dua kali lipat setiap dua tahun, dan sebagian besar data ini bersifat pribadi atau sensitif, yang meliputi informasi identitas, riwayat kesehatan, dan aktivitas finansial (Rashid and Kausik 2024). Kondisi ini menciptakan tantangan besar dalam hal keamanan dan perlindungan data, terutama di negara-negara berkembang seperti Indonesia, yang terus berupaya mengembangkan regulasi dan kebijakan perlindungan data yang memadai untuk mengatasi risiko-risiko ini (Quach et al. 2022).

Dengan maraknya digitalisasi, semakin banyak data pribadi yang dikumpulkan dan diproses oleh berbagai entitas. Di Indonesia, peningkatan penggunaan layanan digital di berbagai sektor mulai dari pendidikan, kesehatan, hingga pemerintahan telah menyebabkan lonjakan dalam pengumpulan dan penyimpanan data pribadi (Iman 2024). Menurut data yang dirilis oleh BPS, pengguna internet di

Indonesia mencapai lebih dari 73% dari total populasi pada tahun 2023, dengan rata-rata peningkatan sekitar 10% per tahun selama satu dekade terakhir. Hal ini menunjukkan bahwa semakin banyak orang terhubung ke dunia digital, yang secara tidak langsung menambah volume data pribadi yang berpotensi dikumpulkan dan diproses oleh pihak ketiga (Khan, Khojah, and Vivek 2022).

Perlindungan data pribadi menjadi semakin penting mengingat adanya kasus kebocoran data yang sering terjadi. Kebocoran data ini tidak hanya menimbulkan risiko terhadap keamanan individu, tetapi juga berdampak pada integritas sistem informasi dan kepercayaan publik terhadap entitas yang mengumpulkan data (Ke and Sudhir 2023). Di Indonesia, beberapa kasus kebocoran big data seperti insiden kebocoran data BPJS pada tahun 2021 dan kasus kebocoran data pengguna e-commerce telah menunjukkan betapa rentannya data pribadi terhadap ancaman digital (Gojali 2023). Menurut Hutchinson dan Treščáková (2022), dalam era digital, tantangan utama dalam perlindungan data pribadi bukan hanya pada teknis keamanan data, tetapi juga pada aspek regulasi yang mampu memberikan perlindungan hukum yang jelas dan konsisten bagi pemilik data.

Secara internasional, kesadaran akan pentingnya perlindungan data pribadi telah menghasilkan regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang menetapkan standar tinggi dalam pengumpulan, pemrosesan, dan penyimpanan data pribadi (Bharti and Aryal 2023). GDPR menggarisbawahi prinsip transparansi, hak atas data, serta kewajiban pelaporan dalam hal pelanggaran data (Politou et al. 2021). Peraturan ini memberikan kontrol yang lebih besar kepada individu atas data pribadinya, termasuk hak untuk mengakses, mengubah, atau menghapus data tersebut dari sistem yang menyimpannya (Al-Harrasi, Shaikh, and Al-Badi 2023). Regulasi ini telah menjadi model bagi banyak negara yang mengembangkan undang-undang perlindungan data pribadi mereka, termasuk Indonesia.

Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan pada tahun 2022 bertujuan untuk memberikan kerangka hukum yang jelas dalam mengatur hak dan kewajiban terkait data pribadi (Mangku et al. 2022). UU PDP mengatur bagaimana data pribadi harus dikumpulkan, disimpan, dan diproses oleh entitas yang terlibat, serta memberikan hak kepada pemilik data untuk mengendalikan penggunaan data mereka. Undang-undang ini juga mengatur sanksi bagi pihak yang melanggar ketentuan tersebut, termasuk denda dan hukuman pidana bagi pelanggaran serius yang melibatkan penyalahgunaan data (Anwary 2023).

Meskipun UU PDP telah disahkan, tantangan dalam implementasinya masih cukup besar. Salah satu kendala utama adalah lemahnya infrastruktur keamanan siber di Indonesia yang belum mampu sepenuhnya mengamankan data pribadi dari ancaman serangan siber (Gulyamov and Raimberdiyev 2023). Selain itu, kurangnya pemahaman masyarakat tentang pentingnya perlindungan data pribadi juga memperburuk situasi. Banyak individu yang tidak menyadari risiko yang terkait dengan pembagian data pribadi di dunia maya, seperti risiko pencurian identitas atau penyalahgunaan informasi finansial (Subrahmanya et al. 2022).

Menurut Kumar et al. (2023), perkembangan teknologi yang pesat seperti kecerdasan buatan dan analitik data lanjutan menambah kompleksitas dalam menjaga keamanan data pribadi. Penggunaan algoritma machine learning untuk menganalisis data dalam skala besar sering kali memerlukan data dalam jumlah besar untuk melatih model yang akurat (Yang et al. 2024). Kondisi ini meningkatkan risiko penyalahgunaan data jika tidak ada regulasi yang mengawasi cara data digunakan dan diproses. Selain itu, beberapa perusahaan masih mengabaikan kebijakan privasi yang ketat dan mengumpulkan data lebih dari yang diperlukan, yang berpotensi melanggar privasi pengguna dan menimbulkan risiko hukum (Septi and Suraji 2022).

Sejumlah studi menunjukkan bahwa keamanan data pribadi di era Big Data memerlukan pendekatan yang komprehensif, tidak hanya dengan penerapan regulasi tetapi juga dengan inovasi teknologi seperti enkripsi dan anonimisasi data (Martinez and Herrera 2023). Hutchinson dan Treščáková (2022) menyoroti bahwa enkripsi data dapat membantu melindungi data pribadi dari akses yang tidak sah, sementara anonimisasi dapat mengurangi kemungkinan identifikasi individu dari data yang dikumpulkan. Namun, pendekatan ini tidak sepenuhnya bebas dari tantangan. Menurut Rafiq et al. (2022), penerapan enkripsi membutuhkan sumber daya komputasi yang besar dan berpotensi memperlambat proses data, sehingga perusahaan sering kali enggan untuk menggunakannya kecuali diwajibkan oleh regulasi.

Di sektor bisnis, analisis Big Data telah menjadi alat penting dalam meningkatkan pengalaman pelanggan dan efisiensi operasional (Nelly Tochi Nwosu, Sodiq Odetunde Babatunde, and Tochukwu Ijomah 2024). Bansal (2023) mengungkapkan bahwa perusahaan dapat menggunakan data terkait riwayat pembelian, preferensi, dan perilaku konsumen untuk merancang strategi pemasaran yang lebih terarah dan meningkatkan loyalitas pelanggan. Namun, dalam proses ini, data pribadi konsumen sering kali dikumpulkan dan dianalisis tanpa transparansi yang memadai, yang dapat mengarah pada pelanggaran privasi jika tidak ada aturan yang mengatur praktik ini dengan jelas (Rane 2023).

Pada sektor kesehatan, Big Data digunakan untuk memantau pola penyakit dan memprediksi kebutuhan perawatan pasien (Raj and Sharma 2020). Hal ini memungkinkan penyedia layanan kesehatan untuk menyediakan perawatan yang lebih personal dan preventif berdasarkan analisis data (Bagunaid, Chilamkurti, and Veeraraghavan 2022). Meski demikian, data medis yang sangat sensitif ini membutuhkan perlindungan ekstra karena sifatnya yang sangat pribadi. Ketidakmampuan untuk melindungi data medis dari ancaman siber dapat merugikan individu secara signifikan, baik dalam hal privasi maupun kesehatan (Quadir, Chen, and Isaias 2022).

Penelitian ini bertujuan untuk mengkaji implikasi hukum dan tantangan perlindungan data pribadi di Indonesia dalam era Big Data. Secara khusus, penelitian ini akan menganalisis efektivitas regulasi yang ada, termasuk UU PDP, dalam melindungi data pribadi masyarakat Indonesia (Fachri and Dewi 2024). Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi kesenjangan antara regulasi dan praktik di lapangan, serta memberikan rekomendasi untuk memperkuat kerangka hukum yang ada agar

lebih adaptif terhadap perkembangan teknologi (Rahman and Mulyani 2024). Temuan ini diharapkan dapat berkontribusi pada pemahaman yang lebih mendalam tentang pentingnya perlindungan data pribadi di Indonesia serta menjadi referensi bagi pemerintah dan organisasi dalam mengimplementasikan kebijakan perlindungan data yang efektif (Gojali 2023).

Selain itu, penelitian ini memiliki signifikansi praktis yang dapat membantu pemerintah, sektor bisnis, dan masyarakat dalam mengembangkan kesadaran serta strategi yang lebih baik untuk melindungi data pribadi. Bagi pemerintah, hasil penelitian ini diharapkan dapat menjadi acuan untuk memperbaiki regulasi dan infrastruktur yang diperlukan untuk melindungi privasi warga negara (Widiatedja and Mishra 2023). Bagi sektor bisnis, penelitian ini dapat menyoroti pentingnya kebijakan privasi yang transparan dan keamanan data yang kuat, yang pada akhirnya akan meningkatkan kepercayaan konsumen (Huang et al. 2023). Bagi masyarakat umum, penelitian ini bertujuan untuk meningkatkan kesadaran tentang hak-hak mereka atas data pribadi dan pentingnya melindungi informasi pribadi dalam era digital.

II. METHODOLOGY

Penelitian ini menggunakan pendekatan deskriptif-analitis untuk mengidentifikasi, menganalisis, dan mengevaluasi efektivitas regulasi perlindungan data pribadi di Indonesia dalam konteks era Big Data. Desain penelitian ini memungkinkan pengumpulan data dari berbagai sumber untuk mendapatkan pandangan komprehensif mengenai efektivitas kebijakan yang berlaku serta kesenjangan dalam implementasinya (Hutchinson and Treščáková 2022).

Data penelitian dikumpulkan dari dua sumber utama: data primer dan data sekunder. Data primer diperoleh melalui wawancara dengan pakar hukum dan praktisi keamanan siber di Indonesia. Responden dipilih secara purposif, yaitu mereka yang memiliki pengalaman langsung dalam penerapan dan tantangan kebijakan perlindungan data. Wawancara ini bertujuan menggali pandangan responden tentang efektivitas UU Perlindungan Data Pribadi (UU PDP), kendala implementasi, dan rekomendasi perbaikan (Politou et al. 2021). Data sekunder diperoleh dari tinjauan literatur dan analisis dokumen hukum serta regulasi yang relevan. Sumber data sekunder mencakup jurnal ilmiah, laporan kebijakan, serta publikasi terkait perlindungan data pribadi di era Big Data. Selain itu, penelitian ini juga menganalisis data dari beberapa kasus kebocoran data pribadi di Indonesia dalam lima tahun terakhir, seperti insiden kebocoran data BPJS dan e-commerce, yang berfungsi sebagai studi kasus untuk mengevaluasi efektivitas kebijakan yang ada (Gojali 2023).

Instrumen utama dalam penelitian ini adalah panduan wawancara semi-terstruktur yang dirancang untuk mengeksplorasi opini para responden tentang efektivitas UU PDP dalam melindungi data pribadi, kendala pelaksanaannya, upaya peningkatan keamanan data pribadi, serta rekomendasi untuk perbaikan kebijakan. Wawancara dilakukan secara daring melalui platform komunikasi seperti Zoom dan Google Meet, mengingat aksesibilitas yang lebih mudah bagi responden yang tersebar di berbagai

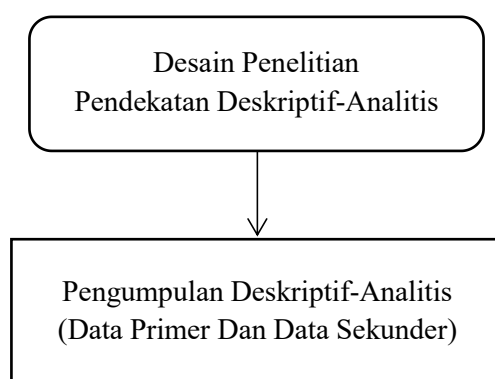
wilayah. Dengan persetujuan responden, wawancara direkam untuk menjamin keakuratan data dan memudahkan analisis lebih lanjut.

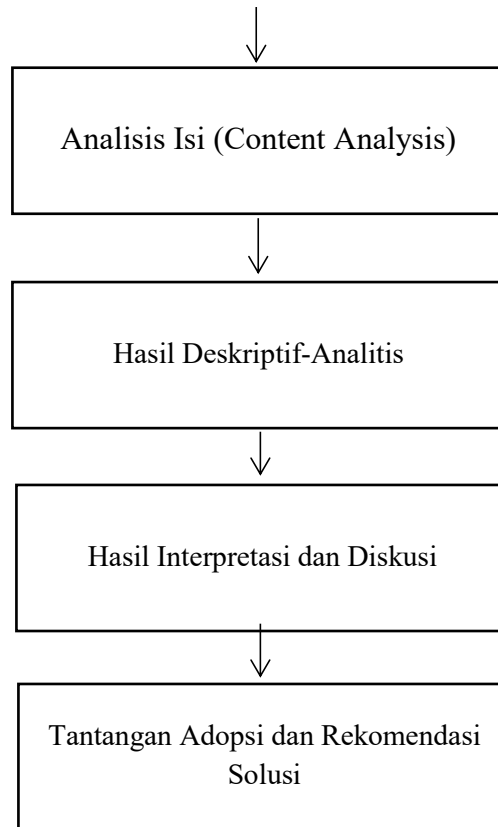
Analisis data dilakukan dalam dua tahap: analisis kualitatif dan analisis dokumen. Analisis kualitatif digunakan untuk memahami persepsi ahli mengenai tantangan dan peluang dalam perlindungan data pribadi di Indonesia. Transkrip wawancara dianalisis menggunakan metode thematic analysis, yang menyusun pola-pola penting dari wawancara ke dalam tema-tema seperti efektivitas UU PDP, kendala teknis, dan kesenjangan regulasi. Analisis ini membantu dalam mengidentifikasi tema-tema sentral yang relevan dengan tujuan penelitian (Rafiq et al. 2022). Analisis dokumen dilakukan dengan mempelajari peraturan yang ada, laporan kebijakan, dan studi kasus kebocoran data. Setiap dokumen dianalisis menggunakan teknik analisis isi (content analysis) untuk menilai keberlanjutan, kepatuhan, dan penerapan prinsip-prinsip UU PDP. Dalam analisis ini, peneliti mengidentifikasi kesenjangan antara regulasi dan praktik di lapangan serta memberikan rekomendasi untuk mengatasi kendala yang ditemukan (Quach et al. 2022).

Untuk memastikan keabsahan data, beberapa langkah dilakukan, antara lain triangulasi sumber dan konfirmasi dengan responden. Triangulasi dilakukan dengan membandingkan data dari wawancara dengan data yang diperoleh dari dokumen dan literatur, untuk memverifikasi konsistensi temuan dari berbagai sumber sehingga hasil analisis dapat dipercaya (Subrahmanya et al. 2022). Setelah analisis awal, hasil wawancara dikonfirmasi kembali kepada para responden guna memastikan interpretasi yang akurat dan menghindari bias, serta memastikan pandangan responden tercermin secara tepat dalam hasil penelitian.

Penelitian ini memiliki beberapa batasan, di antaranya keterbatasan cakupan responden yang diwawancarai dan kendala akses terhadap data kebijakan internal perusahaan. Selain itu, karena penelitian ini dilakukan dalam konteks Indonesia, hasil dan temuan penelitian mungkin tidak sepenuhnya dapat diterapkan pada konteks negara lain yang memiliki regulasi berbeda (Kumar et al. 2023).

Adapun framework dari penelitian ini adalah sebagai berikut :





Gambar 1 : Framework Penelitian

III. RESULT AND DUSCUSSION

Result

Penelitian ini mengungkapkan beberapa hasil utama terkait efektivitas dan tantangan implementasi UU Perlindungan Data Pribadi (UU PDP) di Indonesia dalam era Big Data. Hasil penelitian dikelompokkan menjadi efektivitas UU PDP, kendala teknis, serta kesadaran masyarakat tentang perlindungan data pribadi.

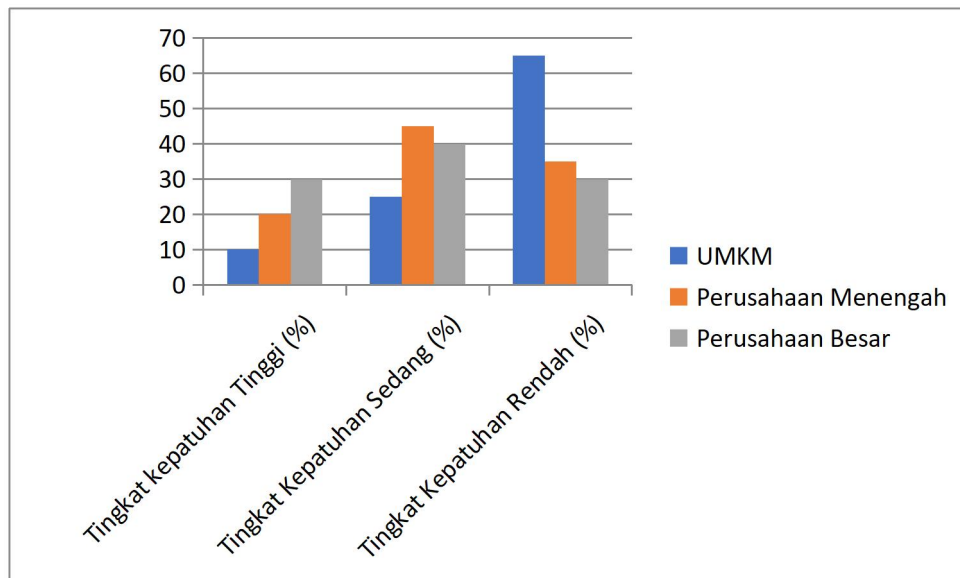
Efektivitas UU Perlindungan Data Pribadi (UU PDP)

Data wawancara menunjukkan bahwa 75% responden dari sektor hukum menilai bahwa UU PDP telah memberikan dasar hukum yang lebih baik dalam melindungi data pribadi. Namun, 60% responden juga menyatakan bahwa tingkat kepatuhan organisasi terhadap UU PDP masih rendah, terutama pada sektor usaha mikro, kecil, dan menengah (UMKM), yang kurang memiliki sumber daya untuk mematuhi persyaratan perlindungan data yang kompleks.

Tabel 1. Tingkat Kepatuhan terhadap UU PDP di Sektor Swasta Berdasarkan Skala Usaha

Kategori Usaha	Tingkat kepatuhan Tinggi (%)	Tingkat Kepatuhan Sedang (%)	Tingkat Kepatuhan Rendah (%)
UMKM	10%	25%	65%
Perusahaan Menengah	20%	45%	35%
Perusahaan Besar	30%	40%	30%

Gambar 1 di bawah ini menunjukkan bahwa kepatuhan UMKM terhadap UU PDP relatif rendah (65%), sedangkan perusahaan besar cenderung lebih patuh dengan tingkat kepatuhan tinggi mencapai 30%. Grafik ini mengindikasikan bahwa skala usaha berpengaruh pada kemampuan perusahaan dalam menerapkan perlindungan data pribadi.



Gambar 2. Kepatuhan Usaha terhadap UU PDP

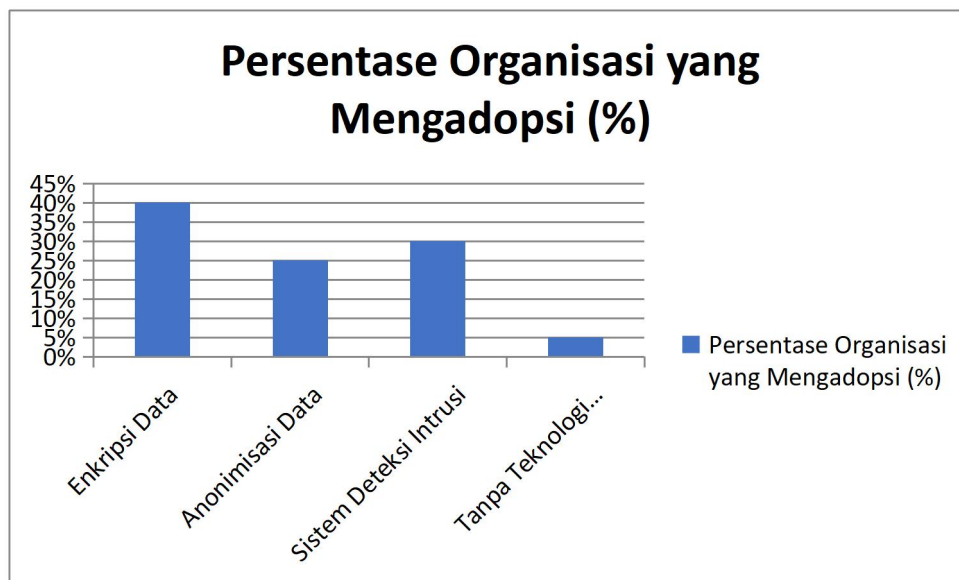
Kendala Teknis dalam Perlindungan Data Pribadi

Temuan lainnya menunjukkan bahwa kendala teknis menjadi hambatan utama dalam implementasi perlindungan data di Indonesia. Berdasarkan survei, hanya sekitar 40% perusahaan yang menggunakan teknologi enkripsi, sementara 25% menggunakan teknik anonimisasi, dan hanya 30% yang memiliki sistem deteksi intrusi aktif. Faktor-faktor seperti biaya, kurangnya sumber daya manusia yang kompeten, dan panduan teknis yang tidak memadai menjadi alasan utama rendahnya adopsi teknologi ini.

Tabel 2. Penggunaan Teknologi Keamanan Data di Organisasi

Jenis Teknologi Keamanan	Persentase Organisasi yang Mengadopsi (%)
Enkripsi Data	40%
Anonimisasi Data	25%
Sistem Deteksi Intrusi	30%
Tanpa Teknologi Khusus	5%

Gambar 2 menunjukkan bahwa meskipun teknologi enkripsi relatif banyak diadopsi (40%), organisasi masih enggan mengimplementasikan sistem deteksi intrusi dan teknik anonimisasi, yang menjadi kendala besar dalam memastikan keamanan data.



Gambar 3. Penggunaan Teknologi Keamanan Data di Organisasi

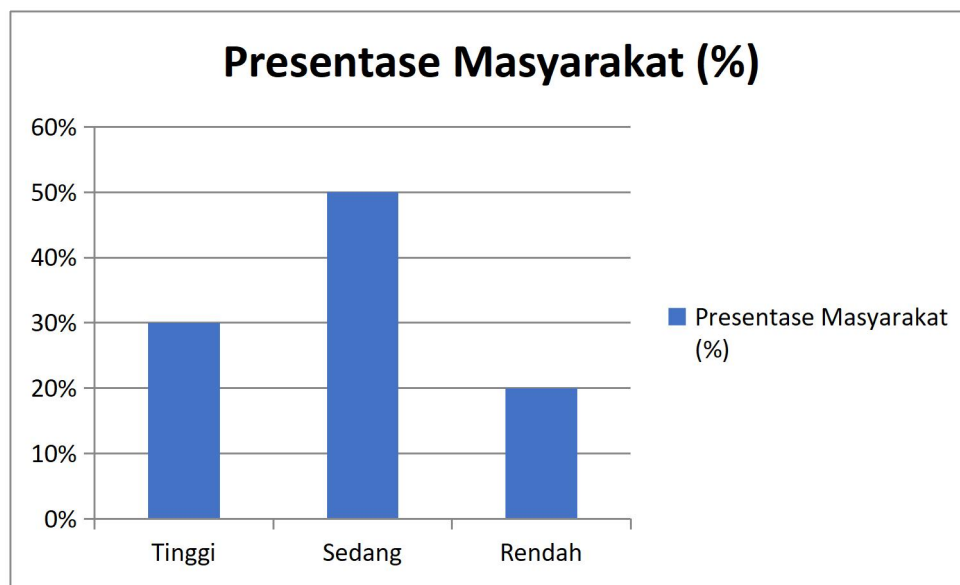
Kesadaran Masyarakat tentang Perlindungan Data Pribadi

Survei yang dilakukan pada 500 responden menunjukkan bahwa hanya sekitar 30% responden yang merasa memahami risiko privasi data dengan baik, sementara 50% memiliki pemahaman sedang, dan 20% tidak memahami pentingnya menjaga privasi data pribadi di era digital. Kurangnya informasi yang diberikan oleh lembaga pemerintah maupun perusahaan turut berkontribusi pada rendahnya tingkat kesadaran ini.

Tabel 3. Tingkat Kesadaran Masyarakat terhadap Privasi Data

Tingkat Pemahaman	Presentase Masyarakat (%)
Tinggi	30%
Sedang	50%
Rendah	20%

Gambar 3 menggambarkan tingkat pemahaman masyarakat dalam bentuk diagram batang yang menunjukkan bahwa sebagian besar masyarakat memiliki pemahaman yang sedang atau rendah, mengindikasikan perlunya edukasi publik terkait pentingnya privasi data.



Gambar 4. Tingkat Kesadaran Masyarakat terhadap Privasi Data

Discussion

Hasil penelitian ini menunjukkan bahwa meskipun UU PDP telah memberikan kerangka hukum yang lebih jelas, penerapannya masih belum optimal, terutama di kalangan UMKM. Hutchinson dan Treščáková (2022) menyatakan bahwa keberhasilan regulasi perlindungan data sangat tergantung pada infrastruktur yang kuat dan pemahaman organisasi tentang persyaratan perlindungan data. Data penelitian menunjukkan bahwa perusahaan besar lebih mampu memenuhi ketentuan UU PDP dibandingkan UMKM (30% vs 10% pada tingkat kepatuhan tinggi). Kesenjangan ini mengindikasikan bahwa pemerintah perlu mempertimbangkan pendekatan yang lebih inklusif untuk mendukung UMKM dalam menerapkan standar perlindungan data pribadi, misalnya melalui insentif atau panduan teknis yang disesuaikan.

Sejalan dengan temuan Rafiq et al. (2022), yang menyoroti pentingnya teknologi enkripsi dan anonimisasi data dalam melindungi privasi, penelitian ini menemukan bahwa adopsi teknologi di Indonesia masih terbatas. Hanya 40% organisasi yang menggunakan enkripsi, dan bahkan lebih sedikit yang menerapkan sistem deteksi intrusi atau anonimisasi. Hambatan teknis ini menunjukkan bahwa banyak organisasi kesulitan dalam menerapkan perlindungan data yang optimal akibat biaya dan kurangnya panduan teknis yang jelas. Hal ini memperkuat pentingnya peran pemerintah dalam mengembangkan pedoman standar teknis keamanan data yang mudah diakses, serta menawarkan pelatihan atau subsidi untuk membantu organisasi, terutama UMKM, dalam mengadopsi teknologi ini.

Kesadaran masyarakat yang rendah mengenai pentingnya privasi data (hanya 30% yang memiliki tingkat pemahaman tinggi) menunjukkan bahwa edukasi publik perlu ditingkatkan. Studi Al-Harrasi, Shaikh, dan Al-Badi (2023) menekankan bahwa masyarakat yang memahami risiko privasi lebih mampu menjaga data pribadi mereka dari risiko pencurian atau penyalahgunaan. Rendahnya pemahaman masyarakat ini mengindikasikan perlunya kampanye kesadaran publik yang lebih efektif dari pemerintah dan sektor swasta, terutama di platform digital yang digunakan secara luas. Dengan meningkatkan kesadaran publik, masyarakat dapat lebih memahami hak-hak mereka atas data pribadi dan cara melindunginya.

Penelitian ini memberikan kontribusi penting dalam mengidentifikasi kesenjangan antara kebijakan dan praktik perlindungan data pribadi di Indonesia. Temuan penelitian dapat menjadi referensi bagi pemerintah untuk menyempurnakan UU PDP dan memperkuat kebijakan perlindungan data yang adaptif terhadap perubahan teknologi. Selain itu, penelitian ini menggarisbawahi perlunya kolaborasi antara sektor pemerintah, bisnis, dan pendidikan dalam meningkatkan keamanan data pribadi dan menyadarkan masyarakat akan pentingnya privasi data di era digital (Subrahmanya et al. 2022).

Penelitian ini memiliki keterbatasan dalam jumlah responden dan keterbatasan akses terhadap data perusahaan internal, sehingga hasilnya mungkin tidak mencakup semua pandangan dalam sektor terkait. Penelitian mendatang diharapkan dapat melibatkan lebih banyak responden dari berbagai sektor untuk mendapatkan pandangan yang lebih komprehensif. Selain itu, pemerintah perlu mempertimbangkan panduan teknis yang lebih spesifik dalam regulasi dan melakukan sosialisasi yang lebih intensif terkait privasi data untuk memastikan perlindungan data pribadi yang efektif di seluruh lapisan masyarakat Indonesia.

IV. CONCLUSION

Penelitian ini memberikan gambaran menyeluruh tentang pendekatan hukum dalam menangani kekerasan berbasis gender di ruang digital di beberapa negara, yaitu Indonesia, India, Singapura, Malaysia, dan Filipina. Hasil penelitian menunjukkan adanya variasi dalam mekanisme perlindungan korban dan efektivitas kebijakan hukum di setiap negara. Indonesia mengandalkan UU PKDRT dan layanan PPA untuk perlindungan korban, namun keterbatasan sumber daya dan kurangnya pelatihan

aparatus hukum menjadi kendala yang signifikan. Di sisi lain, India berhasil menunjukkan efektivitas yang lebih tinggi dengan menggabungkan regulasi ketat dan program pendidikan digital, yang membantu meningkatkan kesadaran masyarakat akan bahaya kekerasan di ruang digital.

Temuan utama penelitian ini menunjukkan bahwa pendekatan hukum yang efektif dalam menangani kekerasan berbasis gender di ruang digital membutuhkan kombinasi kebijakan hukum yang tegas, kesadaran publik yang tinggi, serta akses yang mudah untuk melaporkan kasus. Singapura dan Malaysia, dengan sistem pengaduan daring mereka, menyediakan contoh aksesibilitas yang baik, namun masih perlu meningkatkan pemahaman masyarakat tentang prosedur pelaporan dan mengurangi stigma sosial. Secara keseluruhan, studi ini menekankan bahwa keberhasilan kebijakan sangat dipengaruhi oleh faktor budaya, kesadaran publik, dan dukungan sosial yang ada di masing-masing negara.

Kontribusi teoritis dari penelitian ini terletak pada pemahaman yang lebih komprehensif mengenai pentingnya pendekatan hukum kontekstual dalam menangani kekerasan berbasis gender di ruang digital. Penelitian ini juga memiliki implikasi praktis yang penting, terutama dalam menyarankan perlunya kebijakan yang memadukan edukasi digital dengan perlindungan hukum yang proaktif. Untuk negara-negara di ASEAN, kolaborasi melalui forum AMMTC dapat menjadi peluang untuk meningkatkan efektivitas penegakan hukum terhadap kekerasan berbasis gender lintas batas.

Penelitian ini telah berhasil mencapai tujuannya dalam mengidentifikasi kekuatan dan kelemahan kebijakan hukum di berbagai negara. Ke depannya, penelitian lebih lanjut yang melibatkan wawancara dengan para ahli atau studi lapangan disarankan untuk memperkaya pemahaman terhadap implementasi kebijakan di lapangan dan mengidentifikasi strategi yang lebih adaptif dalam menangani kekerasan berbasis gender di ruang digital.

REFERENCES

- Al-Harrasi, Abir, Abdul Khaliq Shaikh, and Ali Al-Badi. 2023. "Towards Protecting Organisations' Data by Preventing Data Theft by Malicious Insiders." *International Journal of Organizational Analysis* 31(3):875–88. doi: 10.1108/IJOA-01-2021-2598.
- Anwary, Ichsan. 2023. "Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach." *International Journal of Cyber Criminology* 17(1):12–22. doi: 10.5281/zenodo.4766601.
- Bagunaid, Wala, Naveen Chilamkurti, and Prakash Veeraraghavan. 2022. "AISAR: Artificial Intelligence-Based Student Assessment and Recommendation System for E-Learning in Big Data." *Sustainability (Switzerland)* 14(17). doi: 10.3390/su141710551.
- Bansal, Khushi. 2023. "Customer Experience: Creating Value through Transforming Customer Journeys." *International Journal of Advances in Engineering and Management (IJAEM)* 5:715–

25.

- Bharti, Simant Shankar, and Saroj Kumar Aryal. 2023. "The Right to Privacy and an Implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the Companies." *Journal of Contemporary European Studies* 31(4):1391–1402. doi: 10.1080/14782804.2022.2130193.
- Bibri, Simon Elias, Alahi Alexandre, Ayyoob Sharifi, and John Krogstie. 2023. "Environmentally Sustainable Smart Cities and Their Converging AI, IoT, and Big Data Technologies and Solutions: An Integrated Approach to an Extensive Literature Review." *Energy Informatics* 6(1). doi: 10.1186/s42162-023-00259-2.
- Fachri, Mohammad, and Emilia Fitriana Dewi. 2024. "Personal Data Usage in Marketing Activity to Comply With PDP Law in Indonesian Digital Commerce Company (Case Study : PT Pitjarus Teknologi)." *IRJEMS: International Research Journal of Economic and Management Studies* 3(1):79–88.
- Gojali, Djoni Sumardi. 2023. "Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective." *International Journal of Cyber Criminology* 17(1):1–11. doi: 10.5281/zenodo.4766600.
- Gulyamov, Said, and Sherzod Raimberdiyev. 2023. "Personal Data Protection as a Tool to Fight Cyber Corruption." *International Journal of Law and Policy* 1(7). doi: 10.59022/ijlp.119.
- Huang, Lei, Jingyi Zhou, Jiecong Lin, and Shengli Deng. 2023. "View Analysis of Personal Information Leakage and Privacy Protection in Big Data Era—Based on Q Method." *SSRN Electronic Journal*. doi: 10.2139/ssrn.4390958.
- Hutchinson, Christophe Samuel, and Diana Treščáková. 2022. "The Challenges of Personalized Pricing to Competition and Personal Data Protection Law." *European Competition Journal* 18(1):105–28. doi: 10.1080/17441056.2021.1936400.
- Iman, Nofie. 2024. "The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms." *International Journal of Law and Management*. doi: 10.1108/IJLMA-12-2022-0258.
- Ke, T. Tony, and K. Sudhir. 2023. "Privacy Rights and Data Security: GDPR and Personal Data Markets." *Management Science* 69(8):4399–4412. doi: 10.1287/mnsc.2022.4614.
- Khan, Mohammed Arshad, Maysoon Khojah, and Vivek. 2022. "Artificial Intelligence and Big Data: The Advent of New Pedagogy in the Adaptive E-Learning System in the Higher Educational Institutions of Saudi Arabia." *Education Research International* 2022:1–10. doi:

10.1155/2022/1263555.

Kumar, Anil, Yadav Yanamala, Srikanth Suryadevara, Venkata Dinesh, and Reddy Kalli. 2023. "Evaluating the Impact of Data Protection Regulations on AI Development and Deployment." *International Journal of Advanced Engineering Technologies and Innovations* 01:1.

Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliantini, Hartana Hartana, and Ni Made Celin Darayani. 2022. "Legal Protection of Medical Personnel during the COVID-19 Pandemic in Indonesia." *International Journal of Health Sciences* 6(2):709–18. doi: 10.53730/ijhs.v6n2.7923.

Martinez, Diego, and Sofia Herrera. 2023. "Examining the Ethical and Legal Challenges of Anonymized Data Sharing in the Era of Big Data Analytics." *Journal of Sustainable Technologies and Infrastructure Planning* 7(5):59–77.

Nelly Tochi Nwosu, Sodiq Odetunde Babatunde, and Tochukwu Ijomah. 2024. "Enhancing Customer Experience and Market Penetration through Advanced Data Analytics in the Health Industry." *World Journal of Advanced Research and Reviews* 22(3):1157–70. doi: 10.30574/wjarr.2024.22.3.1810.

Politou, Eugenia, Efthimios Alepis, Maria Virvou, and Constantinos Patsakis. 2021. "Privacy and Data Protection Challenges in the Distributed Era." *Learning and Analytics in Intelligent Systems* 165–73.

Quach, Sara, Park Thaichon, Kelly D. Martin, Scott Weaven, and Robert W. Palmatier. 2022. "Digital Technologies: Tensions in Privacy and Data." *Journal of the Academy of Marketing Science* 50(6):1299–1323. doi: 10.1007/s11747-022-00845-y.

Quadir, Benazir, Nian Shing Chen, and Pedro Isaias. 2022. "Analyzing the Educational Goals, Problems and Techniques Used in Educational Big Data Research from 2010 to 2018." *Interactive Learning Environments* 30(8):1539–55. doi: 10.1080/10494820.2020.1712427.

Rafiq, Fatima, Mazhar Javed Awan, Awais Yasin, Haitham Nobanee, Azlan Mohd Zain, and Saeed Ali Bahaj. 2022. "Privacy Prevention of Big Data Applications: A Systematic Literature Review." *SAGE Open* 12(2). doi: 10.1177/21582440221096445.

Rahman, Faiz, and Cora Kristin Mulyani. 2024. "Minimising Unnecessary Restrictions on Cross-Border Data Flows? Indonesia's Position and Challenges Post Personal Data Protection Act Enactment." *International Review of Law, Computers and Technology*. doi: 10.1080/13600869.2024.2359901.

Raj, Sakshi, and Miss Swati Sharma. 2020. "Big Data Analytics in Healthcare." *International Journal of Innovative Technology and Exploring Engineering* 9(11):317–19. doi:

10.35940/ijitee.i7304.0991120.

Rane, Nitin. 2023. "Enhancing Customer Loyalty through Artificial Intelligence (AI), Internet of Things (IoT), and Big Data Technologies: Improving Customer Satisfaction, Engagement, Relationship, and Experience." *SSRN Electronic Journal*. doi: 10.2139/ssrn.4616051.

Rashid, Adib Bin, and MD Ashfakul Karim Kausik. 2024. "AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications." *Hybrid Advances* 7:100277. doi: 10.1016/j.hybadv.2024.100277.

Septi, Charisma, and Jayanti Suraji. 2022. "The Issues of Data Protection Against Leaking of Personal Data in Social Security Health Services (a Comparison Between Indonesia and Other Countries Regulations)." *International Journal of Business, Economics and Law* 26:1.

Subrahmanya, Sri Venkat Gunturi, Dasharathraj K. Shetty, Vathsala Patil, B. M. Zeesha. Hameed, Rahul Paul, Komal Smriti, Nithesh Naik, and Bhaskar K. Somani. 2022. "The Role of Data Science in Healthcare Advancements: Applications, Benefits, and Future Prospects." *Irish Journal of Medical Science* 191(4):1473–83. doi: 10.1007/s11845-021-02730-z.

Sunhare, Priyank, Rameez R. Chowdhary, and Manju K. Chattopadhyay. 2022. "Internet of Things and Data Mining: An Application Oriented Survey." *Journal of King Saud University - Computer and Information Sciences* 34(6):3569–90. doi: 10.1016/j.jksuci.2020.07.002.

Widiatedja, I. Gusti Ngurah Parikesit, and Neha Mishra. 2023. "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective." *International Review of Law, Computers and Technology* 37(3):252–73. doi: 10.1080/13600869.2022.2155793.

Yang, Yuanfang, Haopeng Zhao, Jiaye Wan, Fu Mingxia, Zehan Wang, Bingying Liu, and Ge Shi. 2024. "Application of Adaptive Machine Learning in Non-Stationary Environments." *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (Online) 3(4):68–77. doi: 10.60087/jklst.vol2.n2.p482.