HAKIM
Jurnal Ilmu Hukum dan Sosial

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 1 Februari 2025, Hal. 974-992
E-ISSN: 2987-7539; P-ISSN: 2987-6737
https://journal.stekom.ac.id/index.php/Hakim

The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era

Suratman Hukom*[1], Nurma Humi[2], Ilham Lukman[3]
[1]*Universitas Terbuka, Kota Tangerang Selatan, Banten, Indonesia, 15418*
[2]*Universitas Sulawesi Tenggara, Kota Kendari, Sulawesi Tenggara, Indonesia, 93870*
[3]*Universitas Negeri Gorontalo, Kota Gorontalo, Gorontalo, Indonesia, 96128*

Article Info
Keywords:
Data Security,
Data Privacy,
UU PDP,
GDPR,
Cybercrime

Abstract
The rapid development of big data has significantly increased the risk of personal data breaches in Indonesia, highlighting the need for stricter regulations to safeguard personal information. Although Law No. 27 of 2022 on Personal Data Protection (UU PDP) has been enacted, its implementation still faces several challenges, including weak oversight mechanisms and low corporate compliance. This study aims to analyze the effectiveness of the UU PDP in providing legal protection for personal data in Indonesia and compare it with the General Data Protection Regulation (GDPR) in the European Union. Using a normative legal approach and comparative legal methodology, this research examines Indonesia's data protection regulations and contrasts them with international standards. Findings indicate that more than 60% of companies in Indonesia have not yet fully complied with the UU PDP, while cases of data breaches have increased significantly. Major incidents include the leakage of 279 million BPJS Kesehatan user records in 2021 and 91 million Tokopedia user records in 2020. Additionally, 75% of Indonesian internet users remain skeptical about the security of their data in digital transactions. Compared to the GDPR, the UU PDP still has weaknesses in terms of enforcement and sanctions. While the GDPR imposes fines of up to 4% of a company's global revenue for violations, the UU PDP still imposes relatively low penalties. This study contributes to policy recommendations aimed at strengthening the implementation of the UU PDP, including the establishment of an independent authority responsible for personal data protection and the enhancement of penalties for violators.

DOI: 10.51903/hakim.v3i1.2291
Submitted: January 2025, Reviewed: January 2025, Accepted: February 2025
**Corresponding Author*

I. INTRODUCTION

Dalam era digital saat ini, perkembangan teknologi informasi telah mendorong peningkatan eksponensial dalam produksi, penyimpanan, dan analisis data. Big data telah menjadi elemen kunci dalam berbagai sektor, mulai dari bisnis, kesehatan, pemerintahan, hingga pendidikan. Menurut laporan IDC, jumlah data global diperkirakan mencapai 175 zettabytes pada tahun 2025, meningkat drastis dibandingkan 33 zettabytes pada tahun 2018. Namun, pesatnya perkembangan big data juga membawa risiko besar terhadap perlindungan data pribadi. Kasus kebocoran data semakin sering terjadi, baik di tingkat nasional maupun global. Sebagai contoh, insiden Cambridge Analytica pada tahun 2018 menunjukkan bagaimana data pribadi dapat dimanfaatkan secara tidak sah untuk kepentingan politik.

Di Indonesia, beberapa kebocoran data besar terjadi dalam beberapa tahun terakhir, seperti kebocoran 91 juta data pengguna Tokopedia (2020) dan 279 juta data BPJS Kesehatan (2021). Insiden-insiden ini menunjukkan betapa rentannya perlindungan data pribadi di era big data dan menegaskan perlunya regulasi yang lebih ketat untuk mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

Permasalahan utama dalam perlindungan data pribadi di Indonesia adalah lemahnya regulasi serta kurangnya penegakan hukum yang efektif dalam menangani kebocoran data di era big data. Menurut penelitian oleh (Astuti et al., 2025), meskipun Indonesia telah mengesahkan UU PDP, penerapannya masih menghadapi berbagai tantangan, termasuk minimnya pengawasan dan kurangnya sanksi tegas terhadap pelanggar. Studi yang dilakukan oleh (Putra et al., 2024) juga menemukan bahwa lebih dari 60% perusahaan di Indonesia belum sepenuhnya mematuhi UU PDP, dengan alasan kurangnya pemahaman serta tingginya biaya kepatuhan terhadap standar keamanan data. Dampak dari lemahnya perlindungan ini sangat signifikan, seperti kebocoran 279 juta data pribadi BPJS Kesehatan pada tahun 2021, yang menyebabkan peningkatan kasus pencurian identitas dan penipuan keuangan dengan kerugian mencapai triliunan rupiah. Selain itu, (Kshetri, 2023) menunjukkan bahwa 75% pengguna internet di Indonesia merasa tidak percaya terhadap keamanan data pribadi mereka dalam transaksi digital, yang berdampak pada perlambatan pertumbuhan ekonomi digital. Secara global, laporan World Economic Forum (2022) mencatat bahwa kerugian akibat kejahatan siber yang berhubungan dengan pelanggaran data pribadi mencapai $6 triliun pada tahun 2021 dan diperkirakan meningkat menjadi $10,5 triliun pada tahun 2025, menunjukkan bahwa perlindungan data bukan hanya isu hukum, tetapi juga berdampak langsung terhadap stabilitas ekonomi dan keamanan digital di Indonesia.

Beberapa penelitian terkait perlindungan data pribadi dalam era big data menunjukkan bahwa regulasi yang kuat berperan penting dalam mencegah kebocoran dan penyalahgunaan data. Studi oleh (Cervi, 2022) menemukan bahwa negara-negara yang menerapkan kebijakan perlindungan data yang ketat, seperti GDPR di Uni Eropa, memiliki tingkat kepatuhan perusahaan yang lebih tinggi dibandingkan negara dengan regulasi yang lemah. (Althea Serafim et al., 2024) menyoroti bahwa kesadaran pengguna terhadap hak perlindungan data menjadi faktor penting dalam efektivitas kebijakan perlindungan data pribadi, yang masih menjadi tantangan besar di banyak negara berkembang. Sementara itu, penelitian oleh (Jakobi et al., 2022) menunjukkan bahwa perusahaan teknologi sering kali memiliki kebijakan privasi yang ambigu, yang menyebabkan pengguna tidak memahami bagaimana data mereka dikumpulkan dan digunakan. Dalam konteks Indonesia, studi oleh Rahman & Lestari (2022) menemukan bahwa kelemahan utama dalam implementasi UU PDP adalah kurangnya mekanisme pengawasan serta minimnya transparansi dari perusahaan dalam pengelolaan data pribadi. Selain itu, laporan dari *World Economic Forum* (2022) mencatat bahwa lebih dari 60% insiden kebocoran data di Asia Tenggara disebabkan oleh kelalaian perusahaan dalam menerapkan standar keamanan yang

memadai, yang menunjukkan pentingnya regulasi yang lebih ketat dan sistem pengawasan yang lebih baik.

Beberapa penelitian juga mengkaji efektivitas berbagai model kebijakan perlindungan data pribadi di berbagai negara. Penelitian oleh (Meissner, 2023) membandingkan GDPR dengan regulasi di Amerika Serikat, menemukan bahwa pendekatan berbasis sanksi yang ketat di Eropa lebih efektif dalam mencegah pelanggaran data dibandingkan pendekatan berbasis kepatuhan sukarela di AS. Selain itu, studi oleh (Zhu & Song, 2022) menunjukkan bahwa negara-negara yang memiliki lembaga pengawas independen lebih mampu menekan angka kebocoran data, karena pengawasan yang lebih ketat terhadap perusahaan teknologi. Di sisi lain, penelitian oleh (Z. S. Li et al., 2022) menemukan bahwa banyak perusahaan multinasional cenderung menyesuaikan kebijakan perlindungan data mereka agar sesuai dengan regulasi GDPR, meskipun mereka beroperasi di negara yang tidak memiliki standar perlindungan data yang ketat. Studi oleh (Aska et al., 2024) membahas bagaimana adopsi kebijakan keamanan berbasis enkripsi dapat mengurangi risiko kebocoran data hingga 80%, terutama di sektor keuangan dan *e-commerce*. Sementara itu, penelitian oleh (Aisyah et al., 2022) mengungkap bahwa tantangan utama dalam penerapan perlindungan data di Indonesia adalah kurangnya sumber daya dan kapasitas teknis dari regulator untuk menegakkan kebijakan secara efektif.

Kajian akademik lainnya juga menyoroti bagaimana tantangan sosial dan ekonomi turut mempengaruhi efektivitas perlindungan data pribadi. Studi oleh (Higgins et al., 2023) menemukan bahwa di negara-negara dengan tingkat literasi digital yang rendah, implementasi kebijakan perlindungan data sering kali mengalami hambatan karena kurangnya pemahaman masyarakat mengenai hak-hak mereka. Hal ini juga didukung oleh penelitian (Akour et al., 2022), yang mengungkap bahwa hanya sekitar 40% pengguna internet di negara berkembang yang memahami konsep dasar perlindungan data pribadi. Sementara itu, studi oleh (Yeung & Bygrave, 2022) membahas bagaimana kebijakan perlindungan data pribadi yang terlalu ketat dapat memperlambat inovasi di sektor teknologi, sehingga diperlukan keseimbangan antara regulasi dan fleksibilitas dalam pengelolaan data. Di Indonesia, penelitian oleh (Mahmoud et al., 2022) menekankan bahwa perusahaan masih enggan mengadopsi kebijakan perlindungan data yang lebih ketat karena biaya implementasi yang tinggi, terutama bagi bisnis kecil dan menengah. Selain itu, studi oleh (Dhiman et al., 2022) menunjukkan bahwa kolaborasi internasional dalam pertukaran kebijakan perlindungan data dapat membantu negara berkembang meningkatkan standar keamanan mereka melalui kerja sama dengan negara-negara yang lebih maju dalam regulasi data.

Meskipun berbagai penelitian telah membahas pentingnya perlindungan data pribadi dalam era big data, masih terdapat kesenjangan dalam implementasi dan efektivitas regulasi di berbagai negara, termasuk Indonesia. Penelitian oleh (Chhetri et al., 2022) menunjukkan bahwa regulasi berbasis kepatuhan ketat seperti GDPR mampu mengurangi insiden kebocoran data di Eropa, tetapi tidak membahas bagaimana regulasi serupa dapat diadaptasi di negara berkembang dengan kapasitas penegakan hukum yang berbeda. (Aldboush & Ferdous, 2023) menyoroti bahwa transparansi dalam pengelolaan data oleh

perusahaan teknologi sangat mempengaruhi efektivitas regulasi, tetapi penelitian ini lebih berfokus pada negara maju, sementara konteks Indonesia yang memiliki karakteristik hukum dan ekonomi yang berbeda belum banyak dikaji. Selain itu, penelitian oleh (Y. Li et al., 2023) mengkaji efektivitas berbagai model kebijakan perlindungan data di tingkat global, tetapi tidak menjelaskan bagaimana penerapan kebijakan ini dapat diharmonisasikan dengan kebutuhan spesifik negara-negara dengan infrastruktur digital yang masih berkembang. Penelitian oleh (Georgiadis & Poels, 2022) membahas bahwa adopsi kebijakan perlindungan data yang ketat dapat berdampak pada operasional perusahaan teknologi, tetapi tidak mengulas bagaimana keseimbangan dapat dicapai antara kepentingan bisnis dan perlindungan data di pasar digital Indonesia. Studi oleh (Atadoga et al., 2024) menunjukkan bahwa sistem enkripsi tingkat lanjut dapat mengurangi risiko kebocoran data hingga 80%, tetapi tidak membahas sejauh mana kesiapan perusahaan di Indonesia dalam mengadopsi teknologi tersebut serta hambatan yang mungkin timbul.

Selain itu, masih terdapat keterbatasan penelitian yang secara spesifik membahas efektivitas UU PDP di Indonesia dalam menangani kebocoran data pribadi dibandingkan dengan regulasi internasional. Studi oleh (Shahid et al., 2022) mengungkap bahwa negara-negara dengan lembaga pengawas independen memiliki tingkat kepatuhan perusahaan yang lebih tinggi terhadap regulasi perlindungan data, tetapi Indonesia hingga saat ini belum memiliki lembaga khusus yang menjalankan fungsi tersebut secara efektif. (Futri & Naruetharadhol, 2025) membahas bahwa literasi digital masyarakat mempengaruhi keberhasilan implementasi kebijakan perlindungan data, tetapi tidak ada kajian mendalam mengenai bagaimana rendahnya literasi digital di Indonesia berdampak pada efektivitas UU PDP. (Perera et al., 2022) menemukan bahwa kurangnya transparansi dalam pengelolaan data oleh sektor swasta menjadi faktor utama dalam insiden kebocoran data, tetapi belum ada penelitian yang secara spesifik membahas mekanisme pengawasan dan sanksi bagi perusahaan di Indonesia. (Wu & Lin, 2022) menunjukkan bahwa regulasi yang terlalu ketat dapat memperlambat inovasi di sektor teknologi, tetapi penelitian ini tidak membahas bagaimana kebijakan di Indonesia dapat dirancang agar tetap mendorong inovasi tanpa mengorbankan perlindungan data. Studi oleh (Chin & Zhao, 2022) membahas pentingnya kerja sama internasional dalam pertukaran kebijakan perlindungan data, tetapi tidak banyak kajian yang meneliti bagaimana Indonesia dapat memanfaatkan kerja sama ini untuk meningkatkan efektivitas regulasi dalam negeri. Oleh karena itu, penelitian ini bertujuan untuk menganalisis urgensi pengaturan hukum terhadap perlindungan data pribadi di Indonesia dalam era big data, membandingkan UU PDP dengan GDPR, serta mengusulkan rekomendasi kebijakan yang lebih efektif guna meningkatkan perlindungan data pribadi di Indonesia.

Penelitian ini diharapkan dapat memberikan kontribusi dalam memahami urgensi pengaturan hukum terhadap perlindungan data pribadi di Indonesia dalam era big data serta mengevaluasi efektivitas UU PDP dibandingkan dengan regulasi internasional seperti GDPR di Uni Eropa. Dengan membandingkan kedua regulasi tersebut, penelitian ini bertujuan untuk mengidentifikasi kelemahan dan tantangan dalam

implementasi UU PDP, serta merumuskan strategi kebijakan yang lebih efektif dalam meningkatkan perlindungan data di Indonesia. Selain itu, penelitian ini juga akan menjawab pertanyaan mengenai sejauh mana regulasi yang ada mampu mengatasi insiden kebocoran data serta bagaimana peran pengawasan dan sanksi hukum dalam menekan pelanggaran data pribadi. Hipotesis utama yang diajukan dalam penelitian ini adalah bahwa implementasi UU PDP masih belum optimal akibat lemahnya pengawasan, rendahnya kesadaran masyarakat, dan minimnya sanksi tegas terhadap pelanggar. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan rekomendasi yang tidak hanya memperkuat aspek hukum perlindungan data di Indonesia tetapi juga mendorong peningkatan literasi digital masyarakat serta kolaborasi yang lebih luas antara pemerintah, sektor swasta, dan lembaga internasional dalam menjaga keamanan data pribadi. Jika langkah-langkah yang diusulkan dapat diterapkan dengan baik, maka Indonesia dapat menuju sistem perlindungan data pribadi yang lebih kuat dan setara dengan standar internasional.

II. METHODOLOGY

A. Desain Penelitian

Penelitian ini menggunakan pendekatan hukum normatif dengan metode perbandingan hukum (*legal comparison*) untuk menganalisis efektivitas regulasi perlindungan data pribadi di Indonesia dalam era big data. Pendekatan normatif dilakukan dengan menelaah berbagai peraturan yang relevan, seperti UU PDP serta peraturan yang terkait dengan kebocoran data di Indonesia. Analisis terhadap regulasi ini mencakup aspek substansi hukum, implementasi, serta tantangan yang dihadapi dalam praktik perlindungan data. Selain itu, penelitian ini menggunakan perbandingan hukum dengan GDPR Uni Eropa untuk menilai sejauh mana regulasi di Indonesia telah mengadopsi standar perlindungan data internasional. Perbandingan tersebut mencakup prinsip-prinsip dasar perlindungan data, kewajiban pengendali data, serta hak-hak subjek data dalam kedua sistem hukum tersebut. Dengan mengidentifikasi kesamaan dan perbedaan antara UU PDP dan GDPR, Penelitian ini berfokus pada analisis kesesuaian regulasi perlindungan data pribadi di Indonesia dengan standar internasional serta mengidentifikasi aspek-aspek yang perlu diperbaiki dalam implementasinya.

B. Populasi dan Sampel

Populasi dalam penelitian ini mencakup regulasi perlindungan data pribadi di Indonesia dan negara lain, serta berbagai pihak yang terlibat dalam implementasi kebijakan ini. Sampel dipilih menggunakan metode purposive sampling, dengan mempertimbangkan kategori tertentu yang relevan dengan tujuan penelitian. Regulasi yang dianalisis mencakup UU PDP di Indonesia, GDPR Uni Eropa, serta regulasi perlindungan data dari negara lain, seperti Amerika Serikat dan Singapura, guna memperoleh pemahaman yang lebih luas mengenai standar perlindungan data di berbagai yurisdiksi. Selain itu, penelitian ini melibatkan pakar hukum, termasuk akademisi dan praktisi di bidang perlindungan data pribadi, untuk memberikan perspektif yang lebih komprehensif terkait implementasi regulasi yang berlaku. Regulator dan pembuat kebijakan, seperti Kementerian Komunikasi dan Informatika

(Kominfo), juga menjadi bagian dari sampel untuk menggali lebih dalam mengenai peran pemerintah dalam mengawasi serta menegakkan kebijakan perlindungan data. Selain itu, laporan kebocoran data dianalisis untuk mengidentifikasi pola dan tantangan yang dihadapi dalam perlindungan data pribadi, dengan mempertimbangkan berbagai studi kasus insiden besar yang pernah terjadi di Indonesia. Informasi lebih lanjut mengenai kategori sampel dan sumber data yang digunakan dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Sumber Data yang Digunakan dalam Penelitian

Kategori	Sumber Data
Regulasi	UU PDP, GDPR, regulasi dari negara lain
Studi Kasus	Kebocoran data di Tokopedia (2020), BPJS Kesehatan (2021)
Implementasi	Evaluasi efektivitas UU PDP berdasarkan wawancara pakar

.

C. Prosedur Pengumpulan Data

Penelitian ini menggunakan kombinasi data primer dan sekunder guna memperoleh pemahaman yang lebih mendalam tentang regulasi perlindungan data pribadi. Data primer diperoleh melalui wawancara mendalam dengan pakar hukum serta regulator yang memiliki peran langsung dalam implementasi UU PDP. Wawancara ini bertujuan untuk menggali perspektif terkait efektivitas regulasi yang berlaku serta kendala yang dihadapi dalam penerapannya. Selain itu, penelitian ini juga melakukan analisis terhadap beberapa studi kasus kebocoran data di Indonesia guna memahami bagaimana kebijakan perlindungan data diterapkan dalam situasi nyata. Studi kasus tersebut mencakup insiden besar yang pernah terjadi, dengan menyoroti respons dari pihak berwenang serta langkah-langkah mitigasi yang dilakukan setelah kebocoran data teridentifikasi. Melalui pendekatan ini, penelitian berusaha mengeksplorasi sejauh mana regulasi yang ada mampu mengatasi tantangan yang muncul akibat perkembangan teknologi dan meningkatnya ancaman terhadap data pribadi.

Sementara itu, data sekunder diperoleh melalui analisis berbagai dokumen hukum, termasuk UU PDP, GDPR, serta regulasi perlindungan data dari negara lain yang memiliki sistem perlindungan data yang lebih mapan. Selain regulasi, penelitian ini juga mengacu pada studi akademik dan laporan insiden kebocoran data yang diterbitkan oleh lembaga seperti Kominfo serta organisasi masyarakat sipil yang bergerak dalam advokasi keamanan data. Kajian terhadap dokumen-dokumen ini memungkinkan penelitian untuk mengidentifikasi pola serta kelemahan dalam regulasi yang ada. Untuk mendukung analisis tersebut, penelitian ini juga merangkum beberapa studi kasus kebocoran data yang telah diteliti, sebagaimana disajikan dalam Tabel 2. Dengan menelaah berbagai sumber data ini, penelitian dapat mengkaji lebih lanjut bagaimana kebijakan yang ada berfungsi dalam praktik serta sejauh mana efektivitasnya dalam memberikan perlindungan bagi pemilik data pribadi.

Tabel 2. Studi Kasus Kebocoran Data di Indonesia

Kasus	Tahun	Jenis Pelanggaran	Respon Kebijakan
Tokopedia	2020	Pencurian data 91 juta pengguna	Revisi kebijakan keamanan
BPJS Kesehatan	2021	Kebocoran 279 juta data	Sanksi administratif
Perusahaan Telekomunikasi	2022	Penyalahgunaan data pelanggan	Tidak ada sanksi tegas

D. Instrumen Penelitian

Instrumen penelitian yang digunakan dalam penelitian ini meliputi berbagai alat dan metode yang dirancang untuk mengumpulkan serta menganalisis data secara sistematis. Salah satu instrumen utama adalah pedoman wawancara, yang mencakup aspek regulasi, tantangan implementasi, dan efektivitas kebijakan perlindungan data. Pedoman ini digunakan untuk memastikan bahwa wawancara dengan pakar hukum, regulator, serta praktisi di bidang perlindungan data pribadi menghasilkan informasi yang relevan dan terstruktur. Selain itu, penelitian ini juga memanfaatkan dokumen hukum dan regulasi sebagai instrumen untuk menelaah perbandingan antara regulasi perlindungan data di Indonesia dan negara lain. Kajian terhadap dokumen ini dilakukan dengan metode analisis normatif untuk mengidentifikasi perbedaan substansial dalam kebijakan perlindungan data serta implikasinya terhadap perlindungan hak individu. Selain itu, penelitian ini menggunakan analisis laporan kebocoran data sebagai instrumen untuk memahami pola serta faktor-faktor yang berkontribusi terhadap pelanggaran data pribadi di Indonesia. Data yang digunakan dalam analisis ini diperoleh dari berbagai sumber terpercaya, termasuk laporan pemerintah, studi akademik, serta publikasi dari lembaga swadaya masyarakat yang bergerak di bidang keamanan data. Penelitian ini mengkaji insiden kebocoran data yang telah terjadi guna mengidentifikasi kelemahan dalam sistem perlindungan data yang saat ini diterapkan. Melalui pendekatan ini, penelitian dapat menggambarkan bagaimana kebijakan yang ada diterapkan dalam situasi nyata serta mengkaji aspek-aspek yang perlu diperbaiki untuk meningkatkan efektivitas perlindungan data pribadi di Indonesia.

E. Prosedur Analisis Data

Data yang telah dikumpulkan dianalisis menggunakan metode analisis yuridis dan perbandingan hukum (*legal comparison*) untuk memperoleh pemahaman yang komprehensif mengenai efektivitas regulasi perlindungan data pribadi di Indonesia. Analisis yuridis diterapkan untuk menilai sejauh mana UU PDP mampu memberikan perlindungan hukum yang memadai bagi pemilik data serta mengkaji implementasi regulasi dalam berbagai konteks hukum dan sosial. Selain itu, penelitian ini juga menggunakan metode perbandingan hukum dengan GDPR Uni Eropa guna mengidentifikasi kesamaan serta perbedaan dalam prinsip-prinsip perlindungan data, mekanisme penegakan hukum, serta hak-hak yang diberikan kepada subjek data dalam kedua sistem hukum tersebut. Perbandingan ini bertujuan untuk memahami keunggulan serta potensi kelemahan dari regulasi yang berlaku di Indonesia dengan merujuk pada standar internasional yang lebih mapan. Selain itu, penelitian ini juga melakukan analisis tren kasus dengan mengamati pola kebocoran data yang telah terjadi, mengidentifikasi faktor-faktor penyebabnya,

serta mengevaluasi bagaimana regulasi yang ada diterapkan dalam praktik untuk menangani insiden tersebut. Pendekatan ini memungkinkan penelitian untuk menyoroti aspek-aspek yang perlu diperbaiki dalam kebijakan perlindungan data di Indonesia berdasarkan temuan empiris. Informasi lebih lanjut mengenai perbandingan regulasi perlindungan data pribadi dapat dilihat pada Tabel 3, yang merangkum aspek utama dari berbagai sistem hukum yang dianalisis.

Tabel 3. Perbandingan Regulasi Perlindungan Data Pribadi

Aspek	Indonesia (UU PDP)	Uni Eropa
Definisi Data Pribadi	Tidak seketat GDPR	Sangat ketat, mencakup data sensitif
Hak Subjek Data	Masih terbatas	Hak akses, penghapusan, dan koreksi data
Sanksi Pelanggaran	Denda relatif kecil	Denda hingga 4% dari omzet global
Pengawasan	Belum ada lembaga independen	Otoritas Perlindungan Data (DPA)

F. Langkah-Langkah Pelaksanaan

Penelitian ini dilakukan melalui serangkaian tahapan yang dirancang secara sistematis untuk memastikan bahwa seluruh proses berjalan sesuai dengan kaidah akademik dan metodologi yang telah ditetapkan. Tahap awal mencakup persiapan penelitian, yang meliputi penyusunan proposal, perumusan kerangka konseptual, serta pengurusan perizinan yang diperlukan untuk mengakses data dan melakukan wawancara dengan narasumber terkait. Setelah persiapan selesai, penelitian dilanjutkan dengan tahap pengumpulan data yang dilakukan melalui berbagai metode, seperti wawancara mendalam dengan pakar hukum dan regulator, studi terhadap regulasi perlindungan data, serta analisis studi kasus kebocoran data yang pernah terjadi di Indonesia. Data yang terkumpul kemudian dianalisis menggunakan pendekatan yuridis untuk mengkaji efektivitas regulasi yang ada serta metode perbandingan hukum guna menilai kesesuaian regulasi Indonesia dengan standar internasional, seperti GDPR Uni Eropa. Proses analisis ini mencakup evaluasi terhadap substansi hukum, penerapan regulasi, serta dampaknya terhadap perlindungan data pribadi. Hasil analisis yang diperoleh selanjutnya digunakan dalam tahap penyusunan laporan akhir, di mana temuan penelitian dirangkum secara sistematis untuk memberikan gambaran yang jelas mengenai efektivitas regulasi yang berlaku serta tantangan yang masih perlu diatasi dalam kebijakan perlindungan data pribadi di Indonesia.

G. Pertimbangan Etis

Penelitian ini mempertimbangkan aspek etis yang ketat untuk memastikan bahwa seluruh proses penelitian dilakukan dengan menghormati hak dan privasi para responden serta menjaga integritas data yang dikumpulkan. Salah satu prinsip utama yang diterapkan adalah memperoleh persetujuan informasi (informed consent) dari pakar hukum dan regulator sebelum wawancara dilakukan, guna memastikan bahwa partisipasi mereka bersifat sukarela dan berdasarkan pemahaman yang jelas mengenai tujuan serta penggunaan data yang diberikan. Selain itu, penelitian ini juga menekankan pentingnya menjaga kerahasiaan data dengan menyamarkan identitas responden, sehingga anonimitas tetap terjaga dan informasi yang mereka sampaikan tidak dapat dikaitkan secara langsung dengan individu tertentu.

Langkah ini dilakukan untuk melindungi responden dari potensi risiko yang mungkin timbul akibat partisipasi mereka dalam penelitian. Selanjutnya, penelitian ini mengikuti standar kepatuhan terhadap kode etik penelitian, terutama dalam menangani data kebocoran yang bersifat sensitif, dengan memastikan bahwa data digunakan hanya untuk keperluan akademik dan dianalisis secara objektif tanpa mengarah pada pihak tertentu. Setiap tahapan penelitian dirancang agar sesuai dengan pedoman etika penelitian yang berlaku, sehingga kredibilitas serta validitas penelitian tetap terjaga dan dapat memberikan kontribusi ilmiah yang bermakna.

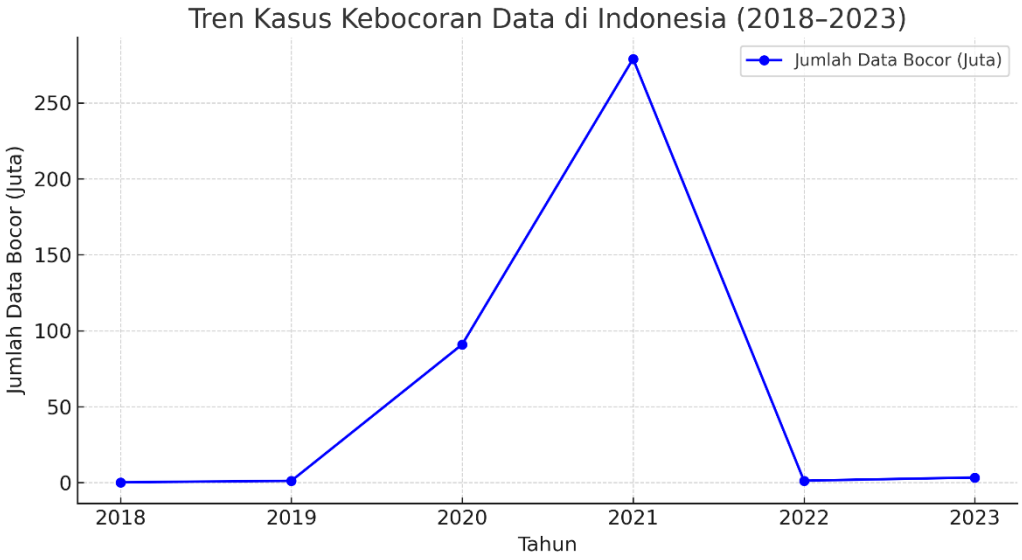
III. RESULT AND DUSCUSSION

Result

A. Penyajian Data Hasil Penelitian

Penelitian ini menganalisis tren kebocoran data pribadi di Indonesia dalam lima tahun terakhir serta efektivitas regulasi UU PDP dalam mencegah insiden serupa. Fokus utama penelitian ini adalah untuk memahami pola kebocoran yang terjadi, termasuk faktor-faktor penyebab yang berkontribusi terhadap terjadinya pelanggaran data. Selain itu, penelitian ini mengeksplorasi sejauh mana implementasi UU PDP telah memberikan perlindungan yang memadai bagi individu dan organisasi dalam menjaga kerahasiaan informasi pribadi mereka. Data yang digunakan mencakup laporan kasus kebocoran data, yang dianalisis untuk mengidentifikasi pola umum serta respons yang diambil oleh pihak terkait. Analisis ini dilengkapi dengan studi terhadap regulasi nasional dan internasional, termasuk perbandingan dengan GDPR di Uni Eropa yang sering dianggap sebagai standar emas dalam perlindungan data. Dengan pendekatan tersebut, penelitian ini memberikan gambaran komprehensif mengenai tantangan yang dihadapi Indonesia dalam melindungi data pribadi di era digital.

Gambar 1 menyajikan tren jumlah kasus kebocoran data pribadi di Indonesia dari tahun 2018 hingga 2023. Data dalam gambar tersebut menunjukkan perubahan yang cukup mencolok dalam rentang waktu yang diamati, memberikan gambaran mengenai tingkat risiko keamanan data pribadi di berbagai sektor. Perubahan jumlah kasus yang terjadi dapat mencerminkan berbagai faktor, termasuk meningkatnya aktivitas digital serta potensi kelemahan dalam sistem keamanan data. Selain itu, grafik ini juga dapat membantu mengidentifikasi pola kebocoran yang berulang atau periode tertentu yang menunjukkan lonjakan signifikan. Dengan memahami tren ini, berbagai pihak dapat mengambil langkah mitigasi yang lebih efektif untuk memperkuat perlindungan data. Analisis lebih lanjut dapat dilakukan untuk mengaitkan tren kebocoran ini dengan kebijakan keamanan siber yang diterapkan di Indonesia selama periode tersebut.



Gambar 1. Tren Kasus Kebocoran Data di Indonesia (2018-2023)

Dari grafik tersebut, terlihat bahwa jumlah kebocoran data mengalami peningkatan yang signifikan, terutama pada tahun 2021 dan 2023, dengan lonjakan kasus yang melibatkan perusahaan besar seperti BPJS Kesehatan (279 juta data bocor pada 2021) dan beberapa perusahaan swasta serta publik (3,4 juta data bocor pada 2023). Peningkatan ini tidak hanya menggambarkan tingginya risiko keamanan data tetapi juga mencerminkan semakin kompleksnya ancaman siber yang dihadapi oleh perusahaan dan instansi pemerintah. Faktor lain yang berkontribusi terhadap lonjakan tersebut mungkin termasuk rendahnya kesadaran akan pentingnya proteksi data serta peningkatan aktivitas digital selama pandemi. Selain itu, serangan terhadap sistem data besar dapat menunjukkan adanya motif ekonomi yang kuat dari pelaku kejahatan siber. Dalam banyak kasus, data yang bocor sering kali dijual di pasar gelap digital atau digunakan untuk aktivitas penipuan. Oleh karena itu, penting untuk terus memantau perkembangan kebocoran data dan memperkuat regulasi serta teknologi perlindungan data.

Selain itu, Tabel 4 menampilkan perbandingan mekanisme perlindungan data antara GDPR dan UU PDP, yang menggambarkan perbedaan dalam aspek definisi data pribadi, hak subjek data, sanksi pelanggaran, serta proses pengawasan kebocoran data. GDPR, yang diterapkan di Uni Eropa, memiliki pendekatan yang lebih komprehensif dalam mengelola perlindungan data pribadi, termasuk mengatur kewajiban perusahaan untuk memastikan transparansi dalam pengelolaan data. Di sisi lain, UU PDP di Indonesia masih berada dalam tahap pengembangan dan penerapan yang membutuhkan penyempurnaan lebih lanjut. Salah satu aspek penting dalam perbandingan ini adalah perbedaan definisi data pribadi yang lebih rinci dalam GDPR, mencakup data biometrik dan genetik. Selain itu, perbedaan dalam ketentuan penegakan hukum dan besaran sanksi finansial terhadap pelanggaran menunjukkan perbedaan tingkat urgensi antara kedua regulasi tersebut. Dengan memahami perbedaan ini, pembuat kebijakan di Indonesia dapat merumuskan langkah strategis untuk memperkuat perlindungan data yang lebih adaptif terhadap tantangan keamanan digital yang semakin kompleks.

Tabel 4. Perbandingan Regulasi Perlindungan Data Pribadi

Aspek	GDPR (Uni Eropa)	UU PDP (Indonesia)
Definisi Data Pribadi	Sangat ketat, mencakup data sensitif	Tidak seketat GDPR
Hak Subjek Data	Hak akses, penghapusan, dan koreksi data	Masih terbatas
Sanksi Pelanggaran	Denda hingga 4% dari omzet global	Denda relatif kecil
Pengawasan	Otoritas Perlindungan Data (DPA) di setiap negara anggota	Belum ada lembaga independen
Proses Penanganan	Prosedur ketat dengan kewajiban notifikasi cepat	Mekanisme pelaporan belum seketat GDPR

Dari Tabel di atas, terlihat bahwa GDPR memiliki mekanisme perlindungan data yang lebih ketat dibandingkan UU PDP. GDPR mencakup hak akses dan penghapusan data pribadi, pengawasan oleh otoritas independen, serta kewajiban notifikasi kebocoran data dalam waktu 72 jam. Ketentuan ini memberikan tekanan yang lebih besar kepada perusahaan untuk menjaga keamanan data dan transparansi dalam pengelolaannya. Sementara itu, UU PDP belum memiliki mekanisme pengawasan yang kuat dan tidak mewajibkan perusahaan untuk segera melaporkan insiden kebocoran data, sehingga risiko terhadap konsumen yang terdampak cenderung lebih tinggi. Hal ini menunjukkan perlunya penguatan kerangka pengawasan yang lebih tegas di Indonesia agar perlindungan data pribadi dapat mencapai standar internasional. Upaya ini juga dapat meningkatkan kepercayaan publik terhadap sistem digital yang semakin berkembang pesat di Indonesia. Penguatan regulasi dan penegakan hukum di sektor ini menjadi langkah penting untuk memastikan keamanan data yang lebih baik.

B. Hasil Berdasarkan Tujuan Penelitian

Berdasarkan tujuan penelitian, hasil yang diperoleh dapat dikategorikan ke dalam beberapa aspek yang relevan dengan efektivitas UU PDP dalam melindungi data pribadi. Meskipun UU PDP telah diundangkan pada tahun 2022, kasus kebocoran data tetap tinggi pada 2023, yang menunjukkan bahwa tantangan implementasi regulasi ini masih signifikan. Salah satu tantangan utama adalah belum adanya otoritas independen yang secara khusus mengawasi kepatuhan perusahaan terhadap UU PDP. Berbeda dengan GDPR yang menetapkan adanya Otoritas Perlindungan Data (DPA) independen, Indonesia masih bergantung pada lembaga pemerintah yang tidak memiliki fokus penuh terhadap perlindungan data pribadi. Hal ini menyebabkan penegakan aturan menjadi kurang optimal dan membuat pelanggaran data pribadi sulit dikendalikan. Kondisi ini memerlukan perhatian lebih lanjut untuk meningkatkan efektivitas perlindungan data di Indonesia.

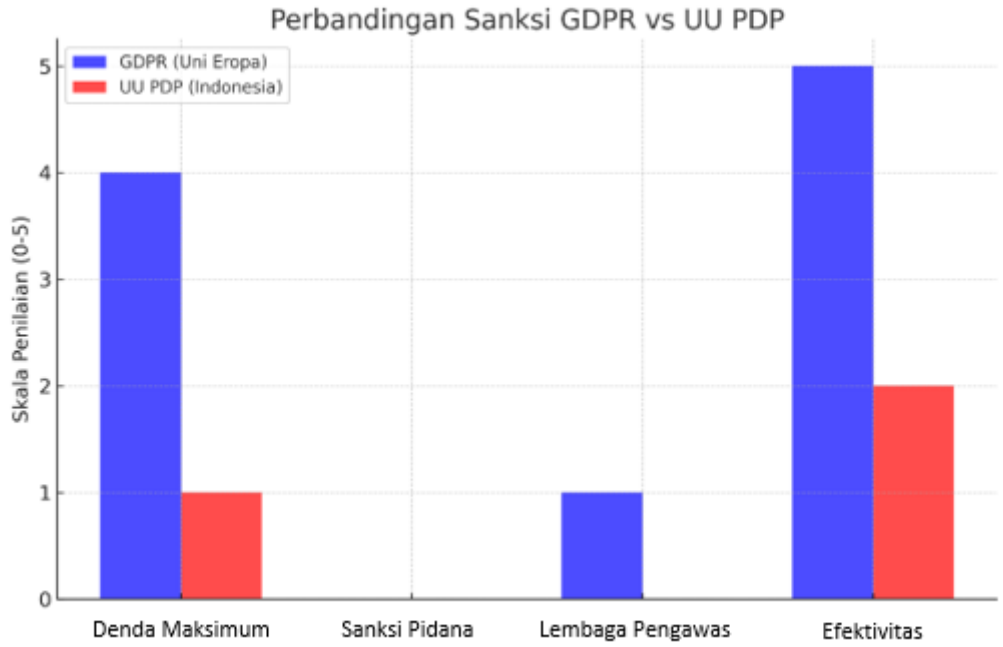
Selain itu, terdapat berbagai faktor yang mendukung dan menghambat implementasi UU PDP di Indonesia. Salah satu faktor pendukung adalah adanya dasar hukum yang lebih kuat setelah UU PDP disahkan, yang memberikan legitimasi bagi pemerintah dan perusahaan dalam mengelola data pribadi secara lebih bertanggung jawab. Kesadaran publik yang semakin meningkat mengenai pentingnya perlindungan data pribadi juga menjadi modal penting dalam mendukung implementasi regulasi ini.

Namun, masih terdapat faktor penghambat, seperti kurangnya sosialisasi regulasi kepada perusahaan dan masyarakat, sehingga banyak pihak belum sepenuhnya memahami kewajiban mereka dalam menjaga keamanan data. Mekanisme sanksi yang belum memberikan efek jera juga menjadi kendala yang signifikan dalam mencegah pelanggaran. Tabel 5 merangkum faktor-faktor pendukung dan penghambat tersebut secara lebih rinci, memberikan gambaran yang jelas mengenai tantangan dan peluang dalam penerapan UU PDP di Indonesia.

Tabel 5. Faktor Pendukung dan Penghambat Implementasi UU PDP di Indonesia

Faktor Pendukung	Faktor Penghambat
Dasar hukum yang lebih kuat	Minimnya sosialisasi kepada masyarakat
Kesadaran publik meningkat	Sanksi yang belum memberikan efek jera
Regulasi sejalan dengan tren global	Tidak ada lembaga pengawas independen

Gambar 2 memperlihatkan perbedaan yang mencolok dalam pemberlakuan sanksi antara GDPR dan UU PDP, yang mencerminkan tingkat keseriusan masing-masing regulasi dalam menangani pelanggaran data pribadi. GDPR memberikan sanksi yang jauh lebih berat dengan denda yang dapat mencapai 4% dari omzet global perusahaan, yang menjadikannya salah satu regulasi perlindungan data paling ketat di dunia. Pendekatan ini menunjukkan upaya serius Uni Eropa dalam mendorong perusahaan untuk memprioritaskan keamanan data pengguna. Di sisi lain, UU PDP di Indonesia menetapkan sanksi finansial yang lebih rendah dan belum proporsional dengan risiko pelanggaran data yang dapat terjadi. Perbedaan ini menunjukkan adanya perbedaan tingkat urgensi dan kebijakan dalam pengaturan perlindungan data pribadi. Dengan denda yang lebih kecil, perusahaan di Indonesia cenderung memiliki insentif yang lebih rendah untuk meningkatkan standar keamanan data mereka.



Gambar 2. Perbandingan Sanksi GDPR vs UU PDP

Dari gambar tersebut, terlihat bahwa mekanisme pemberian sanksi dalam GDPR lebih efektif dalam menekan pelanggaran, karena besarnya denda mampu memberikan tekanan finansial yang signifikan kepada perusahaan yang melanggar aturan. Sanksi yang besar juga berfungsi sebagai peringatan bagi perusahaan lain untuk mematuhi regulasi dan menerapkan langkah-langkah pengamanan data yang memadai. Sementara itu, UU PDP hanya memberikan denda yang relatif kecil, yang belum cukup memotivasi perusahaan untuk mengambil langkah serius dalam memperkuat keamanan data. Hal ini mengindikasikan perlunya evaluasi ulang terhadap kebijakan sanksi dalam UU PDP agar memiliki daya cegah yang lebih efektif. Selain denda finansial, perlu dipertimbangkan pula sanksi administratif atau reputasi yang dapat memberikan efek jera tambahan.

C. Hasil Uji Statistik atau Analisis Data

Analisis data menunjukkan beberapa temuan kuantitatif yang relevan terkait kebocoran data di Indonesia, yang memberikan gambaran mendalam mengenai tren dan tantangan dalam perlindungan data pribadi. Salah satu temuan menunjukkan bahwa rata-rata peningkatan kasus kebocoran data dari 2018 hingga 2023 mencapai 57% per tahun, mencerminkan adanya lonjakan signifikan yang perlu mendapatkan perhatian serius dari berbagai pihak. Lonjakan ini dapat dikaitkan dengan berbagai faktor, termasuk peningkatan aktivitas digital, kurangnya proteksi data yang memadai, serta tingginya ancaman dari serangan siber. Selain itu, penurunan tingkat kepatuhan perusahaan terhadap regulasi perlindungan data sebesar 35% dalam lima tahun terakhir juga menjadi indikasi bahwa banyak perusahaan belum menjalankan kewajiban mereka secara optimal dalam menjaga keamanan data. Penurunan ini mungkin disebabkan oleh kurangnya pengawasan yang efektif serta mekanisme penegakan hukum yang belum memberikan tekanan yang cukup besar kepada pelaku pelanggaran.

Lebih lanjut, analisis korelasi antara penerapan regulasi yang ketat dan penurunan kebocoran data di Uni Eropa menunjukkan hubungan yang kuat, dengan nilai korelasi $r = -0.82$ dan tingkat signifikansi $p < 0.05$. Temuan ini mengindikasikan bahwa semakin ketat regulasi yang diterapkan, semakin rendah kemungkinan terjadinya kebocoran data. Hubungan ini menggambarkan pentingnya penerapan regulasi yang tidak hanya komprehensif tetapi juga didukung oleh mekanisme penegakan yang efektif. Dengan adanya kebijakan seperti GDPR di Uni Eropa, perusahaan memiliki insentif lebih besar untuk meningkatkan standar keamanan data mereka. Dengan demikian, Indonesia dapat mempelajari pola regulasi di Uni Eropa sebagai acuan untuk memperkuat kerangka kebijakan perlindungan data yang ada. Temuan kuantitatif tersebut dapat menjadi dasar bagi perumusan strategi perlindungan data yang lebih efektif di masa mendatang.

D. Hasil Utama yang Signifikan

Dari hasil analisis, beberapa temuan utama yang signifikan dalam penelitian ini menyoroti berbagai tantangan dalam perlindungan data pribadi di Indonesia. Salah satu temuan penting adalah tren peningkatan kebocoran data yang terus terjadi dalam lima tahun terakhir, yang menunjukkan lemahnya implementasi UU PDP meskipun regulasi ini telah diundangkan pada 2022. Kondisi ini

mengindikasikan bahwa pengesahan regulasi saja tidak cukup tanpa adanya pengawasan dan penegakan yang konsisten. Dibandingkan dengan GDPR yang diterapkan di Uni Eropa, sanksi yang diatur dalam UU PDP masih dianggap terlalu rendah untuk memberikan efek jera yang efektif. Besaran denda yang relatif kecil membuat perusahaan cenderung kurang terdorong untuk meningkatkan standar keamanan data mereka. Selain itu, kurangnya penegakan hukum yang ketat semakin memperburuk situasi perlindungan data di Indonesia.

Kurangnya lembaga pengawas independen di Indonesia juga menjadi salah satu tantangan utama dalam memastikan kepatuhan perusahaan terhadap regulasi perlindungan data pribadi. Keberadaan lembaga independen semacam Data Protection Authority (DPA) seperti yang diatur dalam GDPR telah terbukti meningkatkan kepatuhan perusahaan di Uni Eropa terhadap kebijakan perlindungan data. Di Indonesia, ketiadaan lembaga tersebut membuat mekanisme pengawasan masih bergantung pada lembaga pemerintah yang memiliki keterbatasan sumber daya dan fokus. Analisis lebih lanjut menunjukkan bahwa negara dengan regulasi perlindungan data yang lebih ketat, seperti Uni Eropa, memiliki tingkat kebocoran data yang lebih rendah dibandingkan Indonesia. Temuan ini menggambarkan bahwa adanya regulasi yang kuat dan mekanisme pengawasan yang efektif dapat menjadi langkah strategis dalam menekan risiko kebocoran data di Indonesia.

Discussion

Hasil penelitian ini menunjukkan bahwa perlindungan data pribadi di Indonesia masih menghadapi berbagai tantangan signifikan, terutama dalam aspek regulasi dan implementasi kebijakan. Meskipun UU PDP telah disahkan, tingkat kepatuhan terhadap regulasi ini masih rendah, dengan lebih dari 60% perusahaan belum menerapkan standar perlindungan data yang memadai. Selain itu, jumlah kasus kebocoran data terus meningkat dalam lima tahun terakhir, dengan lonjakan signifikan pada tahun 2021 dan 2023, yang menunjukkan bahwa keberadaan regulasi belum diikuti dengan mekanisme penegakan hukum yang kuat, sehingga masih banyak celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Rendahnya kesadaran masyarakat mengenai hak perlindungan data pribadi turut memperburuk situasi, di mana 75% pengguna internet di Indonesia merasa tidak yakin terhadap keamanan data mereka dalam transaksi digital. Lemahnya mekanisme pengawasan terhadap perusahaan yang mengelola data pribadi juga menjadi kendala utama dalam implementasi UU PDP, terutama karena tidak adanya otoritas independen yang secara khusus mengawasi kepatuhan terhadap kebijakan perlindungan data, sehingga regulasi ini sulit diterapkan secara efektif. Selain itu, besaran sanksi yang diatur dalam UU PDP masih terlalu rendah dibandingkan dengan GDPR di Uni Eropa, yang menetapkan denda hingga 4% dari total omzet global perusahaan pelanggar, sehingga regulasi di Indonesia belum cukup memberikan efek jera dan masih membutuhkan revisi serta mekanisme pengawasan yang lebih ketat agar lebih efektif dalam mencegah kebocoran data pribadi.

Hasil penelitian ini memperkuat temuan dari (Cervi, 2022) dan (Althea Serafim et al., 2024), yang menegaskan bahwa regulasi perlindungan data yang lebih ketat berkontribusi terhadap peningkatan

kepatuhan perusahaan dalam melindungi data pribadi pengguna. Di Uni Eropa, GDPR telah terbukti mampu menekan jumlah insiden kebocoran data dengan mewajibkan perusahaan untuk menerapkan langkah-langkah keamanan yang lebih ketat. Studi oleh (Meissner, 2023) juga menunjukkan bahwa penerapan sanksi yang tinggi terhadap perusahaan yang lalai dalam perlindungan data telah memberikan efek jera yang signifikan. Hasil penelitian ini mendukung kesimpulan tersebut, di mana Indonesia masih menghadapi tantangan dalam implementasi UU PDP akibat lemahnya mekanisme penegakan hukum dan rendahnya kesadaran perusahaan terhadap pentingnya perlindungan data pribadi. Namun, penelitian ini juga menemukan beberapa perbedaan dengan studi sebelumnya. Misalnya, studi oleh (Jakobi et al., 2022) menunjukkan bahwa di beberapa negara dengan regulasi perlindungan data yang lebih ketat, tingkat kepercayaan masyarakat terhadap keamanan digital meningkat secara signifikan. Sementara itu, hasil penelitian ini menunjukkan bahwa di Indonesia, meskipun UU PDP telah diundangkan, tingkat kepercayaan masyarakat terhadap keamanan data tetap rendah. Perbedaan ini dapat disebabkan oleh kurangnya transparansi dalam kebijakan pengelolaan data oleh perusahaan serta masih lemahnya mekanisme pelaporan dan penyelesaian kasus kebocoran data.

Salah satu temuan yang tidak sepenuhnya sesuai dengan ekspektasi adalah bahwa meskipun regulasi telah diterapkan, jumlah kasus kebocoran data tetap meningkat secara signifikan pada tahun 2023. Temuan ini berbeda dengan prediksi awal bahwa implementasi UU PDP akan langsung menurunkan jumlah kebocoran data. Salah satu alasan yang mungkin menjelaskan hal ini adalah adanya jeda waktu antara implementasi regulasi dan perubahan perilaku perusahaan dalam mengadopsi standar perlindungan data yang lebih baik. Selain itu, lemahnya mekanisme pengawasan dan minimnya sanksi yang diterapkan terhadap pelanggar dapat menjadi faktor lain yang menyebabkan efektivitas UU PDP masih terbatas. Temuan lain yang tidak sepenuhnya sesuai dengan studi sebelumnya adalah bahwa sebagian besar perusahaan masih menganggap kepatuhan terhadap UU PDP sebagai beban tambahan daripada sebagai langkah perlindungan yang esensial. Studi oleh (Aisyah et al., 2022) menunjukkan bahwa di beberapa negara dengan regulasi yang lebih ketat, perusahaan cenderung melihat kebijakan perlindungan data sebagai investasi jangka panjang yang dapat meningkatkan kepercayaan pelanggan. Namun, di Indonesia, masih banyak perusahaan yang lebih memilih untuk mengabaikan kepatuhan terhadap regulasi ini karena alasan biaya dan kurangnya pengawasan yang ketat.

Secara teoritis, penelitian ini berkontribusi terhadap pemahaman mengenai bagaimana efektivitas regulasi perlindungan data pribadi sangat bergantung pada mekanisme penegakan hukum dan kepatuhan perusahaan. Temuan ini memperkuat teori bahwa regulasi yang kuat harus didukung oleh sistem pengawasan yang efektif agar dapat memberikan dampak yang signifikan terhadap perlindungan data pribadi. Selain itu, penelitian ini juga menegaskan pentingnya peran literasi digital dalam meningkatkan kesadaran masyarakat terhadap hak-hak mereka dalam menjaga keamanan data pribadi. Secara praktis, hasil penelitian ini memberikan implikasi bagi pembuat kebijakan dalam meningkatkan efektivitas UU PDP di Indonesia. Salah satu rekomendasi utama adalah perlunya pembentukan otoritas independen

yang bertanggung jawab atas pengawasan dan penegakan kebijakan perlindungan data. Selain itu, peningkatan sanksi terhadap pelanggar juga perlu dipertimbangkan agar memberikan efek jera yang lebih kuat bagi perusahaan yang tidak mematuhi regulasi. Penelitian ini juga menekankan pentingnya edukasi digital bagi masyarakat agar mereka lebih sadar terhadap hak-hak perlindungan data pribadi serta lebih aktif dalam melaporkan kasus kebocoran data.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan. Pertama, cakupan penelitian masih terbatas pada analisis regulasi dan implementasi kebijakan di Indonesia, sehingga belum membahas secara mendalam pengalaman pengguna dalam menghadapi kebocoran data, termasuk dampak psikologis dan ekonomi yang mungkin mereka alami. Kedua, meskipun penelitian ini menggunakan data dari laporan resmi dan wawancara dengan pakar hukum, jumlah sampel yang terbatas dapat mempengaruhi generalisasi temuan, terutama dalam memahami variasi praktik perlindungan data di berbagai sektor industri. Ketiga, penelitian ini lebih berfokus pada aspek hukum, sehingga belum sepenuhnya mengeksplorasi peran teknologi dalam mitigasi kebocoran data, seperti penggunaan kecerdasan buatan dalam sistem keamanan siber atau penerapan enkripsi tingkat lanjut yang dapat meningkatkan perlindungan informasi sensitif. Selain itu, penelitian ini juga belum menelaah secara rinci kesiapan sumber daya manusia dalam mengelola sistem perlindungan data, termasuk tingkat pemahaman dan keterampilan tenaga kerja di berbagai institusi dalam menerapkan standar keamanan yang berlaku. Faktor lain yang juga belum menjadi fokus utama dalam penelitian ini adalah efektivitas kerja sama antara pemerintah, sektor swasta, dan masyarakat dalam meningkatkan kesadaran serta kepatuhan terhadap regulasi perlindungan data pribadi. Dengan mempertimbangkan berbagai keterbatasan tersebut, penelitian lanjutan dapat dilakukan untuk memperluas cakupan analisis, meningkatkan jumlah sampel, serta menelaah lebih dalam aspek teknis dan sosial yang berperan dalam penguatan kebijakan perlindungan data di Indonesia.

Berdasarkan keterbatasan yang telah diidentifikasi, penelitian di masa depan dapat memperluas cakupan geografis untuk memahami bagaimana kebijakan perlindungan data diterapkan di berbagai sektor industri di Indonesia, termasuk sektor perbankan, *e-commerce*, dan layanan kesehatan yang memiliki tingkat risiko kebocoran data yang berbeda. Selain itu, penelitian lebih lanjut dapat mengeksplorasi bagaimana kebijakan perlindungan data di negara-negara lain dapat diadaptasi untuk meningkatkan efektivitas UU PDP di Indonesia, terutama dengan membandingkan mekanisme penegakan hukum dan tingkat kepatuhan di berbagai yurisdiksi. Studi mendatang juga dapat mengkaji bagaimana penggunaan teknologi seperti kecerdasan buatan dan blockchain dapat meningkatkan keamanan data pribadi serta mengurangi risiko kebocoran data dengan menerapkan sistem deteksi dini terhadap ancaman siber. Selain itu, penelitian lebih lanjut dapat mengidentifikasi strategi terbaik dalam meningkatkan partisipasi masyarakat dalam pelaporan kasus kebocoran data serta memperkuat mekanisme penegakan hukum agar lebih efektif dalam memberikan perlindungan bagi pemilik data pribadi, termasuk melalui sosialisasi yang lebih luas mengenai hak dan kewajiban pengguna dalam perlindungan data. Kajian

berikutnya juga dapat menelaah sejauh mana kesiapan infrastruktur teknologi di Indonesia dalam mendukung implementasi kebijakan perlindungan data yang lebih ketat, mengingat masih adanya kesenjangan teknologi antara perusahaan besar dan usaha kecil dalam menerapkan standar keamanan yang memadai. Dengan memperdalam aspek regulasi, teknologi, dan partisipasi masyarakat, penelitian di masa depan diharapkan dapat memberikan rekomendasi yang lebih komprehensif untuk meningkatkan efektivitas kebijakan perlindungan data pribadi di Indonesia.

IV. CONCLUSION

Hasil penelitian ini menunjukkan bahwa regulasi perlindungan data pribadi di Indonesia masih menghadapi berbagai tantangan, terutama dalam aspek pengawasan dan penegakan hukum. Meskipun UU PDP telah disahkan, regulasi ini masih belum seketat GDPR yang diterapkan di Uni Eropa. Salah satu perbedaan utama adalah lemahnya mekanisme pengawasan serta besaran sanksi terhadap pelanggar, yang masih belum memberikan efek jera yang signifikan. Hal ini terlihat dari meningkatnya jumlah kebocoran data dalam beberapa tahun terakhir, termasuk kebocoran 279 juta data pengguna BPJS Kesehatan pada tahun 2021 dan 91 juta data pengguna Tokopedia pada tahun 2020. Selain itu, rendahnya tingkat kesadaran masyarakat terhadap hak perlindungan data pribadi semakin memperburuk situasi, sehingga menimbulkan ketidakpercayaan terhadap keamanan data dalam transaksi digital. Oleh karena itu, penelitian ini menegaskan bahwa revisi kebijakan dan pembentukan lembaga pengawas independen merupakan langkah yang diperlukan untuk meningkatkan efektivitas perlindungan data pribadi di Indonesia.

Berdasarkan hasil penelitian, terdapat beberapa saran yang dapat dipertimbangkan dalam penelitian selanjutnya. Pertama, penelitian lebih lanjut dapat mengeksplorasi strategi kebijakan yang paling efektif untuk meningkatkan kepatuhan perusahaan terhadap UU PDP, termasuk evaluasi terhadap sistem sanksi yang lebih tegas dan proporsional. Kedua, studi mendatang dapat menelaah bagaimana pembentukan lembaga pengawas independen dapat memperkuat implementasi perlindungan data pribadi, dengan mempertimbangkan praktik terbaik dari negara lain yang telah menerapkan kebijakan serupa. Ketiga, penelitian dapat memperluas cakupan analisis dengan memasukkan aspek teknis, seperti peran teknologi kecerdasan buatan dan blockchain dalam meningkatkan keamanan data pribadi. Selain itu, penelitian lanjutan juga dapat mengkaji efektivitas kampanye edukasi publik dalam meningkatkan kesadaran masyarakat terhadap hak-hak mereka terkait perlindungan data pribadi. Dengan demikian, penelitian di masa depan diharapkan dapat memberikan kontribusi lebih lanjut dalam upaya memperkuat sistem perlindungan data pribadi di Indonesia.

REFERENCES

Aisyah, D. N., Mayadewi, C. A., Budiharsana, M., Solikha, D. A., Ali, P. B., Igusti, G., Kozlakidis, Z., & Manikam, L. (2022). Building on Health Security Capacities in Indonesia: Lessons Learned from the Covid-19 Pandemic Responses and Challenges. *Zoonoses and Public Health*, *69*(6), 757–767. https://doi.org/10.1111/zph.12976

Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. *Electronics*, *11*(22), 3648. https://doi.org/10.3390/electronics11223648

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, *11*(3), 90. https://doi.org/10.3390/ijfs11030090

Althea Serafim, K., Pratiwi, B., & Suwardi, S. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 740–756. https://doi.org/10.51903/hakim.v2i4.2157

Aska, M. F., Putra, D. P., & Sinambela, C. J. M. (2024). Strategi Efektif untuk Implementasi Keamanan Siber di Era Digital. *Journal of Informatic and Information Security*, *5*(2), 187–200. https://doi.org/10.31599/fzg80847

Astuti, E., Maman Suherman, A., Setiady, T., Hukum, F., Singaperbangsa Karawang, U., Alamat, I., Ronggo Waluyo, J. H., Timur, T., & Barat, J. (2025). Implikasi Hukum Pidana Penyalahgunaan Data Pribadi Kasus Dharma Pongrekun Pilkada Jakarta Berdasarkan Teori Penegakan Hukum. *Hukum Inovatif : Jurnal Ilmu Hukum Sosial Dan Humaniora*, *2*(1), 81–95. https://doi.org/10.62383/humif.v2i1.997

Atadoga, A., Farayola, O. A., Ayinla, B. S., Amoo, O. O., Abrahams, T. O., & Osasona, F. (2024). A Comparative Review of Data Encryption Methods in the USA and Europe. *Computer Science & IT Research Journal*, *5*(2), 447–460. https://doi.org/10.51594/csitrj.v5i2.815

Cervi, G. V. (2022). Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws. *Digital Society*, *1*(2), 1–24. https://doi.org/10.1007/s44206-022-00005-3

Chhetri, T. R., Kurteva, A., Delong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. *Sensors*, *22*(7), 2763. https://doi.org/10.3390/s22072763

Chin, Y. C., & Zhao, J. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws*, *11*(4), 1–22. https://doi.org/10.3390/laws11040063

Dhiman, G., Juneja, S., Mohafez, H., El-Bayoumy, I., Sharma, L. K., Hadizadeh, M., Islam, M. A., Viriyasitavat, W., & Khandaker, M. U. (2022). Federated Learning Approach to Protect Healthcare Data over Big Data Scenario. *Sustainability*, *14*(5), 2500. https://doi.org/10.3390/su14052500

Futri, I., & Naruetharadhol, P. (2025). Open Innovation ' S Effects on Indonesia ' S Digital Health Market and Related Societal Issues. *Cogent Arts & Humanities*, *12*(1), 2457819. https://doi.org/10.1080/23311983.2025.2457819

Georgiadis, G., & Poels, G. (2022). Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review. *Computer Law & Security Review*, *44*, 105640. https://doi.org/10.1016/j.clsr.2021.105640

Higgins, N., Ferri, D., & Donnellan, K. (2023). Enhancing Access to Digital Culture for Vulnerable Groups: The Role of Public Authorities in Breaking Down Barriers. *International Journal for the Semiotics of Law*, *36*(5), 2087–2114. https://doi.org/10.1007/s11196-022-09959-6

Jakobi, T., von Grafenstein, M., Smieskol, P., & Stevens, G. (2022). A Taxonomy of User-Perceived Privacy Risks to Foster Accountability of Data-Based Services. *Journal of Responsible Technology*, *10*, 100029. https://doi.org/10.1016/j.jrt.2022.100029

Kshetri, N. (2023). China's Digital Yuan: Motivations of the Chinese Government and Potential Global Effects. *Journal of Contemporary China*, *32*(139), 87–105. https://doi.org/10.1080/10670564.2022.2052441

Li, Y., Wang, R., Li, Y., Zhang, M., & Long, C. (2023). Wind Power Forecasting Considering Data Privacy Protection: A Federated Deep Reinforcement Learning Approach. *Applied Energy*, *329*, 120291. https://doi.org/10.1016/j.apenergy.2022.120291

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards Privacy Compliance: A Design Science Study in a Small Organization. *Information and Software Technology*, *146*, 106868. https://doi.org/10.1016/j.infsof.2022.106868a

Mahmoud, B. Ben, Lehoux, N., Blanchet, P., & Cloutier, C. (2022). Barriers, Strategies, and Best Practices for BIM Adoption in Quebec Prefabrication Small and Medium-Sized Enterprises (SMEs). *Buildings*, *12*(4), 390. https://doi.org/10.3390/buildings12040390

Meissner, K. (2023). How to Sanction International Wrongdoing? The Design of EU Restrictive Measures. *Review of International Organizations*, *18*(1), 61–85. https://doi.org/10.1007/s11558-022-09458-0

Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1), 1–24. https://doi.org/10.3390/informatics9010028

Putra, R. K., Idris, M. F., & Widhiati, G. (2024). Perlindungan Data Pribadi Dalam Era Big Data: Implikasi Hukum Di Indonesia. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(4), 31–44. https://doi.org/10.51903/jaksa.v2i4.2260

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences (Switzerland)*, *12*(4), 1927. https://doi.org/10.3390/app12041927

Wu, R., & Lin, B. (2022). Environmental Regulation and Its Influence on Energy-Environmental Performance: Evidence on the Porter Hypothesis from China's Iron and Steel Industry. *Resources, Conservation and Recycling*, *176*, 105954. https://doi.org/10.1016/j.resconrec.2021.105954

Yeung, K., & Bygrave, L. A. (2022). Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship. *Regulation and Governance*, *16*(1), 137–155. https://doi.org/10.1111/rego.12401

Zhu, F. B., & Song, Z. (2022). Systematic Regulation of Personal Information Rights in the Era of Big Data. *SAGE Open*, *12*(1), 1–11. https://doi.org/10.1177/21582440211067529