Begawan Abioso
(Volume 17, Nomor 1, Juni 2026)
P-ISSN: 1858-2990 I E-ISSN: 2810-0727
Open access at: https://ejournal.hukumunkris.id/index.php/abioso

Perbandingan Normatif Regulasi Perlindungan Data Pribadi Amerika Serikat dan GDPR Uni Eropa dalam Perspektif Transfer Data Lintas Batas

[a] **Josua Ferdinand Sihotang***
[a] Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia

Submitted: 24-04-2026 Revised: 15-05-2026 Accepted: 18-05-2026 Published: 25-05-2026

Abstrak

Perkembangan era digital global telah menjadikan perlindungan data pribadi sebagai isu hukum yang sangat krusial, terutama akibat kemajuan teknologi kecerdasan buatan dan meningkatnya intensitas serangan siber. Pada tahun 2025, rata-rata biaya pelanggaran data tercatat mencapai USD 4,88 juta per insiden. Penelitian ini mengkaji perbandingan normatif antara regulasi perlindungan data pribadi di Amerika Serikat, khususnya *California Consumer Privacy Act, dengan General Data Protection Regulation* (GDPR) Uni Eropa. Kajian tersebut dipilih karena relevansinya terhadap mekanisme transfer data lintas batas serta urgensinya bagi reformasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia, terutama dalam konteks hubungan perdagangan bilateral antara Indonesia dan Amerika Serikat. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan komparatif. Data penelitian bersumber dari bahan hukum sekunder berupa regulasi, jurnal ilmiah, dan laporan yang relevan hingga September 2025. Hasil penelitian menunjukkan adanya perbedaan mendasar antara sistem perlindungan data pribadi Amerika Serikat dan GDPR, khususnya dalam aspek yurisdiksi dan prinsip akuntabilitas. GDPR menerapkan yurisdiksi ekstrateritorial berdasarkan Pasal 3 serta prinsip akuntabilitas proaktif sebagaimana diatur dalam Pasal 35, sedangkan regulasi di Amerika Serikat cenderung bersifat sektoral dan terfragmentasi berdasarkan negara bagian. Perbedaan tersebut menimbulkan konflik norma, kekosongan norma, dan ketidakpastian hukum dalam mekanisme transfer data lintas batas, termasuk dalam implementasi *EU-US Data Privacy Framework*. Penelitian ini merekomendasikan reformasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui penguatan prinsip-prinsip GDPR guna mendukung harmonisasi regulasi global, meningkatkan kepastian hukum, serta mencegah terjadinya pelanggaran data pribadi di era digital.

Kata Kunci: General Data Protection Regulation; Perlindungan Data Pribadi; Transfer Data Lintas Batas.

Abstract

The development of the global digital era has made personal data protection a highly crucial legal issue, particularly due to the advancement of artificial intelligence technology and the increasing intensity of cyberattacks. In 2025, the average cost of a data breach reached USD 4.88 million per incident. This study examines the normative comparison between personal data protection regulations in the United States, particularly the California Consumer Privacy Act, and the European Union's General Data Protection Regulation (GDPR). This topic was selected because of its relevance to cross-border data transfer mechanisms and its urgency for the reform of Indonesia's Law Number 27 of 2022 concerning Personal Data Protection, especially within the context of bilateral trade relations between Indonesia and the United States. This research employs a normative legal method using statutory, conceptual, and comparative approaches. The research data are derived from secondary legal materials, including regulations, academic journals, and relevant reports published up to September 2025. The findings reveal fundamental differences between the personal data protection systems of the United States and the GDPR, particularly regarding jurisdiction and

* **Email koresponden:** josuaferdinand123@gmail.com

accountability principles. The GDPR adopts extraterritorial jurisdiction under Article 3 and a proactive accountability principle as stipulated in Article 35, whereas regulations in the United States tend to be sectoral and fragmented across individual states. These differences create normative conflicts, legal gaps, and legal uncertainty in cross-border data transfer mechanisms, including the implementation of the EU-US Data Privacy Framework. This study recommends reforming Indonesia's Law Number 27 of 2022 concerning Personal Data Protection by strengthening GDPR principles in order to support global regulatory harmonization, enhance legal certainty, and prevent personal data breaches in the digital era.

Keywords: *General Data Protection Regulation; Personal Data Protection Cross Border; Data Transfer.*

A. Pendahuluan

Di era digital yang semakin terintegrasi secara global, perlindungan data pribadi telah menjadi isu krusial yang berkaitan erat dengan aspek ekonomi, keamanan nasional, dan hak asasi manusia. Perkembangan teknologi, seperti kecerdasan buatan (*artificial intelligence/AI*) dan *big data analytics*, yang mampu memproses data dalam jumlah besar dengan kecepatan tinggi, telah meningkatkan risiko pelanggaran privasi secara signifikan. Pada tahun 2025, rata-rata kerugian akibat pelanggaran data secara global mencapai USD 4,88 juta per insiden, meningkat sebesar 9% dibandingkan tahun sebelumnya. Selain itu, diproyeksikan bahwa pada tahun 2025 sekitar 45% organisasi global akan mengalami serangan terhadap rantai pasok perangkat lunak (*software supply chain attack*), yang dalam praktiknya kerap melibatkan transfer data lintas batas (Samin dkk., 2024).

Data pribadi saat ini tidak hanya dipandang sebagai informasi individual, tetapi juga sebagai aset strategis yang mendukung perkembangan inovasi digital, seperti *machine learning* dan *predictive analytics*. Namun demikian, posisi strategis tersebut menjadikan data pribadi sangat rentan terhadap penyalahgunaan. Pada tahun 2024 tercatat sekitar 4.100 kasus kebocoran data publik, dan proyeksi tahun 2025 menunjukkan peningkatan jumlah insiden, termasuk pelanggaran data besar pada Yale New Haven Health System yang berdampak terhadap 5,5 juta individu pada Maret 2025. Perkembangan *generative artificial intelligence* (GenAI), yang diperkirakan akan digunakan oleh 85% perusahaan dalam proses pengambilan keputusan pada tahun 2025, turut memperbesar risiko pelanggaran privasi karena teknologi tersebut sering kali melibatkan pengumpulan dan pemrosesan data tanpa persetujuan yang memadai. Kondisi ini sejalan dengan peningkatan serangan siber global sebesar 30% pada pertengahan tahun 2024, dengan rata-rata mencapai 1.636 serangan per minggu pada setiap organisasi (IBM Security, 2025).

Dalam konteks tersebut, perbandingan normatif antara hukum perlindungan data pribadi di Amerika Serikat dan *General Data Protection Regulation* (GDPR) Uni Eropa menjadi sangat relevan untuk dikaji. Amerika Serikat menerapkan pendekatan perlindungan data yang bersifat sektoral dan fragmentaris melalui regulasi di tingkat negara bagian, sedangkan GDPR merupakan rezim perlindungan data yang bersifat komprehensif dan diterapkan secara seragam di seluruh negara anggota Uni Eropa (Stanford Human-Centered AI, 2025). Perbandingan tersebut penting dilakukan karena kedua rezim hukum tersebut merepresentasikan dua model utama perlindungan data pribadi di dunia yang saling berinteraksi melalui mekanisme transfer data lintas batas dalam skala besar (Austin, 2025).

Urgensi pemilihan tema ini juga didasarkan pada keterlibatan Indonesia dalam berbagai kerja sama perdagangan dengan Amerika Serikat yang mencakup pertukaran data pribadi konsumen. Di samping itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Indonesia secara konseptual banyak mengadopsi prinsip-prinsip yang terdapat dalam GDPR, meskipun implementasinya masih menghadapi

berbagai tantangan. Oleh karena itu, pemahaman yang komprehensif mengenai perbedaan antara pendekatan fragmentaris Amerika Serikat dan pendekatan ketat GDPR diharapkan dapat memberikan kontribusi akademik dan praktis bagi penyempurnaan regulasi perlindungan data pribadi di Indonesia.

Regulasi perlindungan data pribadi di Amerika Serikat yang masih bergantung pada undang-undang di tingkat negara bagian, seperti *California Consumer Privacy Act* (CCPA) yang diperbarui pada Maret 2024, serta berbagai regulasi baru yang diberlakukan pada tahun 2025, antara lain *Delaware Personal Data Privacy Act* dan *Minnesota Consumer Data Privacy Act*, menunjukkan karakteristik sistem hukum yang sektoral dan fragmentaris. Kondisi tersebut berbanding terbalik dengan *General Data Protection Regulation* (GDPR) Uni Eropa yang menerapkan rezim perlindungan data pribadi secara komprehensif dan terintegrasi, serta telah menjatuhkan denda kumulatif sebesar €5,88 miliar hingga Januari 2025. Perbedaan mendasar antara kedua rezim hukum tersebut menimbulkan implikasi signifikan terhadap mekanisme transfer data lintas batas, termasuk terkait keberlakuan *EU-US Data Privacy Framework* (DPF) yang dikonfirmasi oleh Pengadilan Umum Uni Eropa pada 3 September 2025. Situasi tersebut semakin kompleks seiring dengan perkembangan teknologi kecerdasan buatan (*artificial intelligence/AI*) yang membutuhkan alur pertukaran data secara cepat, luas, dan berkelanjutan, namun tetap menuntut adanya jaminan perlindungan hukum yang memadai terhadap data pribadi.

Implikasi transfer data lintas batas menjadi semakin mendesak pada tahun 2025 ketika Pengadilan Umum Uni Eropa kembali menegaskan keberlakuan *EU-US Data Privacy Framework* (DPF) meskipun masih menghadapi berbagai tantangan hukum. Dalam praktiknya, transfer data lintas batas tetap dipandang sebagai "medan ranjau" hukum akibat perbedaan regulasi antara Amerika Serikat dan Uni Eropa. Kompleksitas tersebut diperkuat oleh kebijakan *Bulk Data Rule* Amerika Serikat pada April 2025 yang membatasi transfer data tertentu dari Amerika Serikat ke negara-negara seperti Tiongkok, Rusia, dan beberapa negara lainnya. Selain itu, laporan *IBM X-Force 2025 Threat Intelligence Index* mencatat peningkatan serangan siber sebesar 13% di kawasan Asia-Pasifik (Chance, 2025). Perkembangan teknologi AI, khususnya penggunaan *large language models* (LLM) yang memerlukan dataset dalam jumlah besar, turut memperburuk permasalahan perlindungan data lintas batas. Laporan *Stanford HAI AI Index 2025* bahkan menunjukkan adanya peningkatan legislasi AI sebesar 21,3% di 75 negara sejak tahun 2023, termasuk lahirnya tiga *Executive Order* Presiden Donald Trump pada Juli 2025 terkait pembangunan infrastruktur AI di Amerika Serikat yang turut memengaruhi pengelolaan dan transfer data sensitif (Jain, 2025).

Pemilihan judul penelitian ini juga dimaksudkan sebagai bahan pertimbangan dalam upaya penyempurnaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia. Regulasi tersebut masih menghadapi sejumlah kelemahan, antara lain keterlambatan pembentukan Badan Perlindungan Data Pribadi (BPDP) serta pengaturan sanksi yang belum memiliki sifat ekstrateritorial. Sanksi administratif dalam UU PDP hanya dibatasi paling tinggi sebesar 2% dari pendapatan tahunan pelanggar, berbeda dengan *General Data Protection Regulation* (GDPR) yang dapat mengenakan denda hingga 4% dari total omzet global perusahaan (Lim & Oh, 2025).

Pertama, terdapat konflik norma antara regulasi perlindungan data pribadi di Amerika Serikat yang bersifat fragmentaris dengan GDPR yang menerapkan standar perlindungan secara ketat dan komprehensif. Regulasi di Amerika Serikat masih bergantung pada

undang-undang negara bagian, seperti *California Consumer Privacy Act* (CCPA) yang diperbarui pada tahun 2024, serta regulasi baru di negara bagian Delaware dan Minnesota pada tahun 2025. Ketentuan tersebut berpotensi bertentangan dengan prinsip yurisdiksi ekstrateritorial sebagaimana diatur dalam Pasal 3 GDPR yang mensyaratkan adanya perlindungan setara dalam mekanisme transfer data lintas batas. Kondisi tersebut menimbulkan ketidakpastian hukum dalam implementasi *EU-US Data Privacy Framework* (DPF) yang keberlakuannya kembali ditegaskan oleh Pengadilan Umum Uni Eropa pada September 2025 (Tschider dkk., 2024).

Konflik norma tersebut juga tampak pada ketidaksinkronan mekanisme sanksi antara kedua rezim hukum. GDPR memberikan kewenangan pengenaan denda administratif hingga 4% dari total omzet global perusahaan, sedangkan penegakan hukum di Amerika Serikat masih bersifat sektoral melalui Federal Trade Commission (FTC). Perbedaan pendekatan tersebut berdampak signifikan terhadap mekanisme transfer data lintas batas, sebagaimana tercermin dalam kasus Meta dan TikTok, serta semakin kompleks dengan berkembangnya teknologi kecerdasan buatan (*artificial intelligence*/AI) (Skillcast, 2025).

Kedua, kekaburan norma muncul pada definisi "perlindungan setara" (*adequate level of protection*) sebagaimana diatur dalam Pasal 45 GDPR mengenai *adequacy decisions*, yang memiliki pengaturan lebih eksplisit dibandingkan regulasi perlindungan data pribadi di Amerika Serikat. Ambang batas pemrosesan data, seperti ketentuan 100.000 konsumen dalam *California Consumer Privacy Act* (CCPA) dan regulasi negara bagian Minnesota, menimbulkan ketidakpastian dalam proses verifikasi transfer data lintas batas, khususnya setelah diberlakukannya *Bulk Data Rule* Amerika Serikat pada April 2025. Kekaburan norma tersebut semakin diperparah oleh kebutuhan teknologi kecerdasan buatan (*artificial intelligence*/*AI*) terhadap akses data *real-time* lintas negara yang hingga kini belum didukung pedoman federal yang jelas dan seragam di Amerika Serikat (Wilson, 2022).

Ketiga, kekosongan norma dalam sistem perlindungan data pribadi Amerika Serikat disebabkan oleh belum adanya undang-undang federal yang komprehensif hingga tahun 2025. Kondisi tersebut menimbulkan celah penegakan hukum yang tidak ditemukan dalam GDPR, yang memberikan kewenangan penjatuhan sanksi administratif hingga €20 juta atau sebesar 4% dari omzet global tahunan perusahaan. Kekosongan norma ini menimbulkan risiko yang signifikan terhadap mekanisme transfer data lintas batas serta pengolahan *dataset* berskala besar untuk pengembangan teknologi kecerdasan buatan.

Keempat, terdapat implementasi hukum yang tidak sepenuhnya selaras dengan norma serta terjadinya tumpang tindih pengaturan dalam rezim perlindungan data pribadi Amerika Serikat. Regulasi di tingkat negara bagian, seperti Delaware dan New Jersey, kerap mengalami irisan pengaturan dengan regulasi federal sektoral, misalnya *Health Insurance Portability and Accountability Act* (HIPAA). Kondisi tersebut berbeda dengan mekanisme penegakan GDPR yang lebih terkoordinasi melalui *European Data Protection Board* (EDPB). Tumpang tindih norma tersebut semakin memperburuk implikasi hukum terhadap transfer data lintas batas, terutama di tengah pesatnya perkembangan teknologi kecerdasan buatan. Oleh karena itu, berbagai persoalan tersebut menunjukkan pentingnya analisis komparatif sebagai dasar penyusunan rekomendasi reformasi terhadap Undang-Undang Perlindungan Data Pribadi di Indonesia (Sulubara dkk., 2025).

Dalam penelitian ini, penulis menggunakan lima artikel ilmiah sebagai tinjauan pustaka guna mendukung analisis perbandingan normatif mengenai hukum perlindungan data pribadi (PDP) di Amerika Serikat (AS), khususnya *California Consumer Privacy Act* (CCPA) beserta berbagai regulasi negara bagian lainnya, dengan *General Data Protection Regulation*

(GDPR) Uni Eropa. Analisis tersebut difokuskan pada implikasi pengaturan terhadap mekanisme transfer data lintas batas serta relevansinya bagi pengembangan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia.

Pertama, penulis mengacu pada artikel ilmiah karya Ruben de Bruin berjudul *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence* (2022) (De Bruin, 2022). Dalam artikel tersebut, de Bruin membahas secara kritis perbandingan rezim perlindungan data p ribadi Uni Eropa melalui GDPR dengan sistem perlindungan data di Amerika Serikat. Fokus utama kajian tersebut terletak pada perbedaan filosofi regulasi, di mana GDPR menempatkan perlindungan data pribadi sebagai bagian dari hak individu dan martabat demokratis, sedangkan Amerika Serikat cenderung memandang individu sebagai "konsumen privasi" dalam mekanisme pasar data. Perbedaan paradigma tersebut menimbulkan implikasi signifikan terhadap mekanisme transfer data internasional.

Temuan utama dalam artikel tersebut menunjukkan bahwa perbedaan pendekatan regulasi antara Uni Eropa dan Amerika Serikat menyebabkan harmonisasi transfer data lintas batas menjadi sulit diwujudkan, meskipun perkembangan teknologi digital global menuntut adanya kerangka regulasi yang interoperabel. Kebaruan yang ditawarkan dalam penelitian de Bruin terletak pada analisis bahwa divergensi regulasi tidak semata-mata disebabkan oleh perbedaan filosofi hukum, melainkan juga dipengaruhi oleh trajektori perkembangan ekonomi data di masing-masing yurisdiksi. Selain itu, artikel tersebut merekomendasikan model konvergensi melalui penguatan portabilitas data dan instrumen hukum persaingan usaha untuk mengatasi dominasi perusahaan teknologi besar (*big tech*).

Relevansi artikel tersebut dengan penelitian yang dilakukan penulis terletak pada kesamaan objek kajian, yaitu perbandingan regulasi perlindungan data pribadi antara Amerika Serikat dan GDPR Uni Eropa, serta potensi konvergensi kedua sistem hukum tersebut. Kajian tersebut menjadi landasan dalam menganalisis konflik norma dan implikasi hukum terhadap transfer data lintas batas. Adapun perbedaannya, penelitian ini tidak hanya berhenti pada analisis komparatif bilateral, melainkan juga berupaya merumuskan model harmonisasi regulasi perlindungan data pribadi di Indonesia yang bersifat *hybrid*. Kebaruan (*novelty*) penelitian ini terletak pada formulasi Model Harmonisasi PDP Indonesia berbasis prinsip-prinsip GDPR yang adaptif terhadap sistem pluralistik sebagaimana diterapkan di Amerika Serikat, sehingga lebih sesuai dengan karakteristik sistem hukum Indonesia yang mengakomodasi otonomi daerah serta kebutuhan untuk menyeimbangkan perlindungan data yang ketat dengan fleksibilitas pengembangan ekonomi digital.

Artikel ilmiah kedua ditulis oleh Elias Aidun dengan judul *Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations* (2025) (Aidun, 2025). Artikel tersebut membahas perkembangan lanskap regulasi perlindungan data pribadi di Amerika Serikat dan Uni Eropa, khususnya perbandingan antara *General Data Protection Regulation* (GDPR) dan *California Consumer Privacy Act* (CCPA), termasuk tantangan transfer data lintas batas serta beban kepatuhan bagi pelaku usaha internasional. Kebaruan yang ditawarkan dalam artikel tersebut terletak pada integrasi studi kasus pasca-*Schrems II* serta usulan model hibrida antara Amerika Serikat dan Uni Eropa sebagai upaya menjembatani kesenjangan regulasi perlindungan data pribadi. Relevansi artikel tersebut dengan penelitian ini terletak pada kesamaan pembahasan mengenai perbedaan regulasi perlindungan data pribadi antara Amerika Serikat dan GDPR beserta implikasinya terhadap transfer data lintas batas dan

aspek kepatuhan hukum. Adapun perbedaannya, penelitian ini tidak hanya berfokus pada perspektif bisnis transatlantik, melainkan mengarahkan analisis pada konteks negara berkembang, khususnya Indonesia. Kebaruan penelitian ini terletak pada perumusan model harmonisasi perlindungan data pribadi Indonesia yang tidak hanya mengadopsi prinsip-prinsip GDPR, tetapi juga mengakomodasi sistem pluralistik sebagaimana diterapkan di Amerika Serikat, sehingga lebih adaptif dan realistis untuk diterapkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang hingga saat ini masih menghadapi berbagai kekosongan norma.

Artikel ilmiah ketiga ditulis oleh M.N.I. Khan dengan judul *Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices* (2025) (Khan, 2025). Artikel tersebut menyajikan tinjauan sistematis menggunakan metodologi PRISMA 2020 terkait transfer data lintas batas di berbagai yurisdiksi. Kebaruan yang ditawarkan dalam penelitian tersebut terletak pada identifikasi kesenjangan penelitian mengenai evaluasi empiris efektivitas penegakan hukum di luar kawasan Global Utara, serta dorongan terhadap penguatan kerja sama lintas batas dan pembentukan perjanjian pengakuan timbal balik (*mutual recognition agreements*). Relevansi artikel tersebut dengan penelitian ini terletak pada pembahasan mengenai fragmentasi hukum, transfer data lintas batas, dan pengaruh GDPR terhadap perkembangan regulasi di berbagai yurisdiksi. Perbedaannya, penelitian ini tidak berhenti pada pemetaan kesenjangan hukum secara global, melainkan mengembangkan temuan tersebut menjadi rekomendasi kebijakan yang lebih konkret melalui formulasi Model Harmonisasi Perlindungan Data Pribadi Indonesia berbasis GDPR yang adaptif terhadap sistem pluralistik. Model tersebut diharapkan mampu mengisi kekosongan norma sekaligus mendukung reformasi Undang-Undang Perlindungan Data Pribadi di Indonesia.

Artikel ilmiah keempat yang dijadikan rujukan dalam penelitian ini adalah karya C. Tschider, M. C. Compagnucci, dan T. Minssen berjudul *The New EU-US Data Protection Framework's Implications for Healthcare* (2024) (Tschider dkk., 2024). Artikel tersebut menganalisis implikasi *EU-US Data Privacy Framework* (DPF) terhadap sektor kesehatan, khususnya terkait efektivitas komitmen Amerika Serikat dalam membatasi akses otoritas keamanan nasional terhadap data pribadi. Kebaruan yang ditawarkan dalam artikel tersebut terletak pada analisis mendalam mengenai kompleksitas standar teknis dan organisasi antara kedua yurisdiksi dalam pengelolaan data sensitif. Relevansi artikel tersebut dengan penelitian ini terletak pada pembahasan mengenai mekanisme transfer data lintas batas berdasarkan EU-US DPF. Adapun perbedaannya, penelitian ini tidak hanya berfokus pada sektor kesehatan, melainkan memperluas cakupan analisis ke konteks perlindungan data pribadi secara umum. Kebaruan penelitian ini terletak pada upaya mengadaptasi pembelajaran dari mekanisme DPF ke dalam model harmonisasi perlindungan data pribadi Indonesia yang menggabungkan kekuatan yurisdiksi ekstrateritorial GDPR dengan fleksibilitas pendekatan pluralistik, sehingga dapat memperkuat implementasi Pasal 56 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terkait persyaratan perlindungan setara dalam transfer data internasional.

Artikel ilmiah terakhir yang menjadi rujukan penelitian ini adalah karya G. Buckley, T. Caulfield, dan I. Becker berjudul *How Might the GDPR Evolve? A Question of Politics, Pace and Punishment* (2024) (Buckley dkk., 2024). Artikel tersebut mengevaluasi perkembangan dan arah evolusi GDPR dengan menitikberatkan pada dinamika politik, kecepatan penegakan hukum, dan efektivitas penerapan sanksi. Kebaruan yang ditawarkan artikel tersebut terletak pada analisis kritis mengenai "budaya penghukuman" (*culture of punishment*) dalam rezim GDPR, serta prediksi mengenai adaptasi regulasi tersebut terhadap perkembangan

teknologi di masa mendatang. Relevansi artikel tersebut dengan penelitian ini terletak pada kontribusinya sebagai landasan teoritis dalam menganalisis aspek akuntabilitas, penegakan hukum, dan efektivitas sanksi dalam perbandingan hukum perlindungan data pribadi. Perbedaannya, penelitian ini tidak hanya membahas evolusi GDPR secara teoritis, tetapi juga mengembangkan implikasinya ke dalam konteks reformasi hukum nasional. Kebaruan penelitian ini terletak pada penggunaan perspektif tersebut untuk merumuskan model harmonisasi perlindungan data pribadi yang lebih holistik bagi Indonesia, termasuk rekomendasi pembentukan badan pengawas independen yang kuat serta penguatan mekanisme sanksi yang lebih efektif, guna mengatasi kelemahan pengaturan sanksi dalam Undang-Undang Perlindungan Data Pribadi yang masih relatif terbatas.

Secara analitis, penelitian ini memiliki perbedaan mendasar dibandingkan dengan lima penelitian terdahulu. Studi-studi sebelumnya pada umumnya bersifat deskriptif-komparatif (De Bruin, 2022); (Aidun, 2025), berupa tinjauan sistematis yang luas (Khan, 2025), maupun analisis sektoral dan spesifik (Tschider dkk., 2024); (Buckley dkk., 2024). Sementara itu, penelitian ini diposisikan sebagai kajian perbandingan hukum normatif yang lebih mendalam dengan fokus pada regulasi perlindungan data pribadi di Amerika Serikat dan *General Data Protection Regulation* (GDPR) Uni Eropa. Penelitian ini secara khusus menyoroti berbagai persoalan hukum konkret, meliputi konflik norma, kekosongan norma, kekaburan norma, serta tumpang tindih norma yang timbul akibat fragmentasi sistem regulasi di Amerika Serikat. Adapun kebaruan utama penelitian ini terletak pada analisis normatif yang komprehensif disertai pembahasan mengenai implikasi praktis terhadap mekanisme *EU-US Data Privacy Framework*, serta perumusan rekomendasi konkret bagi penyempurnaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia.

B. Metode

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) yang bersifat kualitatif. Metode penelitian hukum normatif digunakan karena penelitian ini berfokus pada analisis terhadap norma hukum, prinsip-prinsip hukum, serta sistem hukum yang terkandung dalam regulasi perlindungan data pribadi. Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*).

Pendekatan perundang-undangan (*statute approach*) digunakan untuk mengkaji secara sistematis ketentuan-ketentuan yang terdapat dalam bahan hukum primer, meliputi *California Consumer Privacy Act* (CCPA) beserta perubahannya, berbagai undang-undang perlindungan data pribadi di negara bagian Amerika Serikat, *General Data Protection Regulation* (GDPR), *EU-US Data Privacy Framework* (DPF), serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia. Pendekatan konseptual (*conceptual approach*) digunakan untuk menganalisis konsep-konsep dasar dalam perlindungan data pribadi, seperti yurisdiksi teritorial dan ekstrateritorial, akuntabilitas sektoral dan proaktif, serta prinsip-prinsip perlindungan data yang meliputi transparansi, tanggung jawab, dan perlindungan setara. Selanjutnya, pendekatan perbandingan (*comparative approach*) digunakan untuk membandingkan sistem hukum perlindungan data pribadi Amerika Serikat yang bersifat fragmentaris dan sektoral dengan sistem GDPR yang bersifat komprehensif dan ekstrateritorial. Perbandingan tersebut dilakukan secara fungsional dan normatif guna

menemukan persamaan, perbedaan, konflik norma, kekosongan norma, serta implikasi hukumnya.

Selain itu, penelitian ini juga menggunakan pendekatan kasus (*case approach*) untuk menganalisis sejumlah kasus penting, seperti putusan *Schrems II*, konfirmasi keberlakuan *EU-US Data Privacy Framework* oleh Pengadilan Umum Uni Eropa pada September 2025, serta berbagai kasus sanksi administratif GDPR terhadap perusahaan teknologi besar.

Bahan hukum dalam penelitian ini diklasifikasikan ke dalam tiga jenis. Pertama, bahan hukum primer yang terdiri atas peraturan perundang-undangan dan regulasi resmi, meliputi GDPR (*Regulation (EU) 2016/679*), CCPA (*California Civil Code* § 1798.100 dan seterusnya), berbagai undang-undang perlindungan data pribadi negara bagian di Amerika Serikat, *EU-US Data Privacy Framework*, *Executive Order* 14086, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kedua, bahan hukum sekunder berupa literatur ilmiah, seperti jurnal, buku, laporan resmi, termasuk *IBM Cost of a Data Breach Report 2025*, *Stanford AI Index 2025*, laporan *Clifford Chance*, serta artikel ilmiah lain yang relevan dengan objek penelitian. Ketiga, bahan hukum tersier berupa kamus hukum, ensiklopedia, dan berbagai sumber penjelasan resmi lainnya yang mendukung pemahaman terhadap bahan hukum primer dan sekunder.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*). Analisis bahan hukum dilakukan menggunakan metode interpretasi hukum yang meliputi interpretasi gramatikal, yaitu penafsiran berdasarkan makna harfiah ketentuan peraturan perundang-undangan, serta interpretasi sistematis dengan menempatkan norma hukum dalam keseluruhan sistem hukum yang berlaku.

Analisis bahan hukum dilakukan secara normatif-preskriptif. Secara normatif, penelitian ini mengidentifikasi persamaan, perbedaan, konflik norma, kekosongan norma, serta tumpang tindih norma dalam regulasi perlindungan data pribadi. Sementara itu, secara preskriptif penelitian ini merumuskan rekomendasi kebijakan (*ius constituendum*) bagi penyempurnaan regulasi perlindungan data pribadi di Indonesia. Teknik analisis perbandingan dilakukan menggunakan metode *functional equivalence* untuk membandingkan fungsi dan efektivitas kedua sistem hukum dalam memberikan perlindungan terhadap data pribadi di era digital.

C. Hasil dan Pembahasan

C.1 Perbedaan Normatif Perlindungan Data Pribadi AS dan GDPR Uni Eropa

Perbandingan normatif antara rezim perlindungan data pribadi di Amerika Serikat dan *General Data Protection Regulation* (GDPR) Uni Eropa tidak hanya menunjukkan perbedaan teknis dalam pengaturan regulasi, tetapi juga mencerminkan perbedaan filosofi hukum yang bersifat fundamental. Amerika Serikat menganut pendekatan *market-oriented privacy* yang memandang data pribadi sebagai komoditas dalam mekanisme pasar bebas, sedangkan GDPR menerapkan *rights-based approach* yang menempatkan perlindungan data pribadi sebagai bagian yang tidak terpisahkan dari hak asasi manusia dan martabat individu (*human dignity*).

Dalam aspek yurisdiksi, hukum perlindungan data pribadi di Amerika Serikat bersifat teritorial dan cenderung fragmentaris. Sebagai contoh, *California Consumer Privacy Act* (CCPA) hanya berlaku di negara bagian California dan diterapkan terhadap pelaku usaha yang memenuhi ambang batas tertentu, yaitu memiliki pendapatan tahunan lebih dari 25

juta USD, memproses data pribadi sedikitnya 100.000 konsumen, atau memperoleh 50% pendapatan dari penjualan data pribadi sebagaimana diatur dalam CCPA § 1798.140. Pendekatan tersebut merupakan manifestasi dari prinsip federalisme Amerika Serikat yang memberikan otonomi luas kepada masing-masing negara bagian dalam membentuk regulasi perlindungan data pribadi (Hoofnagle dkk., 2019).

Berbeda dengan pendekatan tersebut, GDPR menerapkan yurisdiksi ekstrateritorial yang luas sebagaimana diatur dalam Pasal 3 GDPR. Regulasi ini berlaku terhadap pengendali maupun prosesor data yang berada di luar wilayah Uni Eropa apabila mereka menawarkan barang atau jasa kepada subjek data di Uni Eropa atau melakukan pemantauan terhadap perilaku subjek data yang berada di wilayah Uni Eropa. Pendekatan ini didasarkan pada *effects doctrine* dalam hukum internasional serta prinsip perlindungan hak asasi manusia yang bersifat universal.

Perbedaan yurisdiksi tersebut memiliki implikasi praktis yang sangat signifikan. Perusahaan teknologi besar asal Amerika Serikat pada praktiknya harus mematuhi standar GDPR secara global, meskipun di dalam yurisdiksi domestiknya hanya tunduk pada regulasi negara bagian yang relatif lebih fleksibel. Kondisi tersebut menimbulkan *regulatory asymmetry* yang tidak hanya meningkatkan beban biaya kepatuhan (*compliance cost*), tetapi juga menciptakan ketidakpastian hukum dalam praktik transfer data pribadi lintas batas negara.

Prinsip akuntabilitas merupakan salah satu pilar utama dalam *General Data Protection Regulation* (GDPR). Pasal 5 ayat (2) GDPR secara tegas menegaskan bahwa pengendali data bertanggung jawab untuk mematuhi prinsip-prinsip pemrosesan data serta wajib mampu membuktikan (*able to demonstrate*) kepatuhan terhadap prinsip-prinsip tersebut. Implementasi prinsip akuntabilitas tersebut diwujudkan melalui berbagai instrumen, antara lain kewajiban penunjukan *Data Protection Officer* (DPO) sebagaimana diatur dalam Pasal 37 GDPR, pelaksanaan *Data Protection Impact Assessment* (DPIA) terhadap pemrosesan data yang berisiko tinggi berdasarkan Pasal 35 GDPR, serta kewajiban pencatatan seluruh aktivitas pemrosesan data sebagaimana diatur dalam Pasal 30 GDPR.

Sebaliknya, prinsip akuntabilitas dalam sistem perlindungan data pribadi di Amerika Serikat cenderung bersifat reaktif dan sektoral. *California Consumer Privacy Act* (CCPA) lebih menitikberatkan pada perlindungan hak konsumen, seperti hak untuk mengakses, menghapus, serta melakukan *opt-out* terhadap penjualan data pribadi. Namun demikian, regulasi tersebut tidak membebankan kewajiban proaktif yang ketat sebagaimana diatur dalam GDPR, seperti kewajiban pelaksanaan DPIA maupun penunjukan DPO secara mandatory. Selain itu, mekanisme penegakan hukum di Amerika Serikat masih sangat bergantung pada *Federal Trade Commission* (FTC) yang bersifat *case-by-case*, serta kewenangan *state attorneys general* di masing-masing negara bagian.

Dari perspektif teori hukum, perbedaan tersebut dapat dijelaskan melalui konsep *accountability* dan *proportionality*. GDPR menerapkan prinsip akuntabilitas proaktif yang sejalan dengan paradigma perlindungan data pribadi sebagai hak fundamental (*fundamental rights*). Sementara itu, pendekatan Amerika Serikat lebih menekankan prinsip *notice and choice* yang bercorak liberal dan berorientasi pasar (*market-oriented approach*). Pendekatan GDPR juga dinilai lebih selaras dengan prinsip *proportionality* dalam hukum hak asasi manusia, karena mewajibkan dilakukannya penilaian risiko sebelum proses pemrosesan data dilakukan.

Secara kritis, pendekatan fragmentaris yang diterapkan di Amerika Serikat berpotensi menimbulkan fenomena *race to the bottom*, yaitu kondisi ketika negara bagian saling berlomba

menawarkan regulasi yang lebih longgar guna menarik investasi ekonomi digital. Sebaliknya, GDPR berhasil membentuk standar minimum global (*Brussels Effect*) yang memengaruhi perkembangan regulasi perlindungan data pribadi di berbagai negara.

Bagi Indonesia, kedua model regulasi tersebut memberikan pelajaran yang signifikan dalam penguatan sistem perlindungan data pribadi nasional. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang saat ini masih berorientasi pada yurisdiksi teritorial, memiliki mekanisme akuntabilitas yang belum optimal, serta pengaturan sanksi yang relatif terbatas, memerlukan reformasi hukum yang lebih komprehensif. Dalam konteks tersebut, penulis merekomendasikan penerapan pendekatan *hybrid* yang adaptif dalam reformasi UU PDP Indonesia, yaitu melalui adopsi prinsip yurisdiksi ekstrateritorial dan akuntabilitas proaktif sebagaimana diterapkan dalam *General Data Protection Regulation* (GDPR) guna memperkuat perlindungan hak privasi masyarakat. Di sisi lain, reformasi tersebut juga perlu mengakomodasi fleksibilitas sektoral sebagaimana diterapkan di Amerika Serikat agar selaras dengan karakteristik otonomi daerah dan kebutuhan pengembangan ekonomi digital nasional. Selain itu, penguatan peran Badan Perlindungan Data Pribadi (BPDP) sebagai otoritas independen yang efektif dan berwenang menjadi aspek penting dalam menjamin optimalisasi pengawasan dan penegakan hukum perlindungan data pribadi di Indonesia.

C.2 Isu Hukum Transfer Data Lintas Batas antara Regulasi AS dan GDPR

Fragmentasi regulasi perlindungan data pribadi di Amerika Serikat yang sangat bergantung pada undang-undang di tingkat negara bagian telah menimbulkan berbagai persoalan hukum yang kompleks. Berbeda dengan *General Data Protection Regulation* (GDPR) yang bersifat komprehensif, seragam, dan berorientasi pada perlindungan hak asasi manusia, sistem perlindungan data pribadi di Amerika Serikat merefleksikan pertentangan antara filosofi *market-oriented privacy* dengan *rights-based approach* sebagaimana dianut oleh GDPR. Konflik norma menjadi isu yang paling menonjol akibat fragmentasi regulasi tersebut. Regulasi di Amerika Serikat yang bersifat sektoral dan teritorial, seperti *California Consumer Privacy Act* (CCPA) yang diperbarui pada Maret 2024 melalui penambahan ketentuan mengenai audit keamanan siber, serta regulasi baru seperti *Delaware Personal Data Privacy Act* dan *Minnesota Consumer Data Privacy Act* tahun 2025, hanya berlaku dalam yurisdiksi masing-masing negara bagian. Ketentuan tersebut berhadapan secara langsung dengan prinsip ekstrateritorial sebagaimana diatur dalam Pasal 3 GDPR, yang mewajibkan setiap pengendali maupun prosesor data, termasuk perusahaan yang berbasis di Amerika Serikat, untuk memenuhi standar perlindungan data yang setara apabila memproses data pribadi penduduk Uni Eropa. Konflik tersebut tampak nyata dalam mekanisme transfer data lintas batas yang menimbulkan ketidakpastian hukum berkepanjangan dalam pelaksanaan *EU-US Data Privacy Framework* (DPF), meskipun keberlakuannya telah ditegaskan oleh Pengadilan Umum Uni Eropa pada September 2025. Kondisi tersebut menunjukkan adanya pertentangan antara pendekatan federalisme di Amerika Serikat dengan prinsip kesatuan dan universalitas perlindungan data yang dianut GDPR (Prastyanti dkk., 2022).

Kekaburan norma terutama muncul dalam penafsiran konsep "perlindungan setara" sebagaimana diatur dalam Pasal 45 GDPR mengenai *adequacy decisions*. GDPR telah memberikan definisi dan kriteria yang relatif eksplisit, sedangkan di Amerika Serikat terdapat perbedaan ambang batas antarnegara bagian, seperti ketentuan pemrosesan data terhadap 100.000 konsumen dalam CCPA dan regulasi Minnesota. Kekaburan norma tersebut semakin kompleks dengan diberlakukannya *Bulk Data Rule* Amerika Serikat pada

April 2025 yang membatasi transfer data tertentu ke negara-negara tertentu. Dalam konteks transfer data lintas batas, kondisi tersebut menimbulkan kesulitan dalam proses verifikasi kepatuhan serta menciptakan tingkat *legal uncertainty* yang tinggi. Perkembangan teknologi kecerdasan buatan (*artificial intelligence/AI*) yang memerlukan pemrosesan data secara *real-time* lintas batas turut memperburuk situasi tersebut, terutama karena belum adanya pedoman yang jelas dan seragam di tingkat federal Amerika Serikat terkait tata kelola perlindungan data pribadi.

Kekosongan norma merupakan kelemahan struktural yang paling mendasar dalam sistem perlindungan data pribadi di Amerika Serikat. Hingga tahun 2025, Amerika Serikat masih belum memiliki undang-undang federal yang komprehensif dan menyeluruh mengenai perlindungan data pribadi. Kondisi tersebut mengakibatkan jutaan warga di negara bagian yang belum memiliki regulasi khusus mengalami keterbatasan perlindungan hukum terhadap data pribadi mereka. Situasi ini sangat berbeda dengan *General Data Protection Regulation* (GDPR) yang menerapkan sanksi administratif secara tegas hingga €20 juta atau sebesar 4% dari omzet tahunan global sebagaimana diatur dalam Pasal 83 GDPR, serta berlaku secara seragam di seluruh negara anggota Uni Eropa. Kekosongan norma tersebut menimbulkan risiko sistemik terhadap mekanisme transfer data lintas batas, khususnya dalam pengolahan dataset berskala besar untuk pengembangan *large language models* (LLM) dan berbagai aplikasi kecerdasan buatan lainnya. Secara teoretis, kondisi tersebut menunjukkan kelemahan pendekatan liberal yang terlalu bergantung pada mekanisme pasar dan pola penegakan hukum yang bersifat reaktif (Asmadi dkk., 2023).

Tumpang tindih norma terjadi akibat adanya persinggungan pengaturan antara berbagai undang-undang negara bagian dengan regulasi federal yang bersifat sektoral. Salah satu contohnya terlihat pada potensi tumpang tindih antara undang-undang perlindungan data baru di Delaware dan New Jersey pada tahun 2025 dengan regulasi federal seperti *Health Insurance Portability and Accountability Act* (HIPAA) di sektor kesehatan. Di sisi lain, penegakan GDPR dilaksanakan secara lebih terkoordinasi melalui *European Data Protection Board* (EDPB), yang pada tahun 2025 menunjukkan peningkatan intensitas penegakan hukum (*enforcement surging*). Berbeda dengan sistem tersebut, penegakan hukum di Amerika Serikat masih sangat bergantung pada *state attorneys general* yang memiliki karakteristik dan tingkat penegakan berbeda di setiap negara bagian. Kondisi tumpang tindih norma ini tidak hanya menyebabkan *overcompliance* bagi perusahaan multinasional, tetapi juga menciptakan celah penegakan hukum di sejumlah wilayah. Pada akhirnya, keadaan tersebut memperbesar risiko serta ketidakpastian hukum dalam transfer data lintas batas, khususnya di tengah pesatnya perkembangan teknologi kecerdasan buatan.

C.3 Implikasi Perbedaan Regulasi AS-Uni Eropa terhadap Transfer Data dan Reformasi UU Perlindungan Data Pribadi

Perbedaan pendekatan regulasi perlindungan data pribadi antara Amerika Serikat yang bersifat fragmentaris dengan *General Data Protection Regulation* (GDPR) yang komprehensif dan memiliki yurisdiksi ekstrateritorial tidak hanya menimbulkan persoalan internal dalam masing-masing sistem hukum, tetapi juga memberikan implikasi yang signifikan terhadap mekanisme transfer data lintas batas. Kondisi tersebut tercermin secara nyata dalam kerangka *EU-US Data Privacy Framework* (DPF) yang saat ini menjadi instrumen utama dalam pengaturan transfer data antara Amerika Serikat dan Uni Eropa.

EU-US Data Privacy Framework sebagai pengganti *Privacy Shield* pasca-putusan *Schrems II* dibentuk untuk menjembatani kesenjangan regulasi antara kedua yurisdiksi. Kerangka

tersebut mengandalkan mekanisme sertifikasi mandiri perusahaan-perusahaan di Amerika Serikat serta komitmen pemerintah Amerika Serikat melalui *Executive Order* 14086 untuk membatasi akses otoritas intelijen terhadap data pribadi. Akan tetapi, efektivitas kerangka tersebut masih dipandang rentan karena fondasi regulasi perlindungan data di Amerika Serikat yang bersifat sektoral dan fragmentaris belum sepenuhnya memenuhi standar "perlindungan setara" (*adequate level of protection*) sebagaimana dipersyaratkan dalam Pasal 45 GDPR.

Dari perspektif teori hukum, persoalan tersebut dapat dianalisis melalui teori hak privasi (*privacy as a fundamental right*) dan teori perlindungan data. GDPR menempatkan perlindungan data pribadi sebagai hak fundamental yang harus dijamin secara proaktif, konsisten, dan berkelanjutan tanpa dipengaruhi oleh lokasi geografis perpindahan data. Sebaliknya, pendekatan Amerika Serikat yang bertumpu pada mekanisme *notice and choice* serta pola penegakan sektoral cenderung mencerminkan pendekatan liberal yang berorientasi pada mekanisme pasar. Ketidakseimbangan antara kedua pendekatan tersebut berpotensi bertentangan dengan prinsip *proportionality* dalam hukum hak asasi manusia, karena risiko terhadap hak privasi subjek data di Uni Eropa tidak diimbangi dengan jaminan perlindungan yang setara dalam sistem hukum Amerika Serikat.

Secara praktis, fragmentasi regulasi perlindungan data pribadi di Amerika Serikat menimbulkan sejumlah permasalahan mendasar dalam mekanisme transfer data lintas batas. Pertama, muncul ketidakpastian hukum karena perusahaan-perusahaan di Amerika Serikat wajib mematuhi regulasi yang berbeda pada setiap negara bagian, sedangkan *General Data Protection Regulation* (GDPR) menuntut penerapan standar perlindungan data yang seragam dan konsisten. Kedua, lemahnya prinsip akuntabilitas proaktif menyebabkan sulitnya pembuktian kepatuhan secara berkelanjutan terhadap kewajiban perlindungan data pribadi. Ketiga, ketiadaan undang-undang federal yang komprehensif menjadikan *EU-US Data Privacy Framework* (DPF) bersifat rentan dan berpotensi menghadapi tantangan hukum di masa mendatang, sebagaimana tercermin dari konfirmasi Pengadilan Umum Uni Eropa pada September 2025 yang tetap memperoleh kritik dari kelompok advokasi privasi (Martono dkk., 2025).

Dalam perspektif *cyber law*, kondisi tersebut mencerminkan belum tercapainya harmonisasi regulasi di tengah arus globalisasi digital. Perbedaan rezim hukum antara Amerika Serikat dan Uni Eropa tidak hanya meningkatkan biaya kepatuhan (*compliance cost*) bagi pelaku usaha, tetapi juga menghambat kelancaran arus data yang dibutuhkan dalam pengembangan teknologi kecerdasan buatan. Selain itu, kondisi tersebut turut meningkatkan risiko kebocoran data dan penyalahgunaan data pribadi. Bagi Indonesia, implikasi dari perbandingan kedua rezim hukum tersebut memiliki relevansi yang signifikan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang hingga saat ini masih bersifat teritorial, memiliki mekanisme akuntabilitas yang relatif lemah, serta sanksi administratif yang terbatas, yaitu paling tinggi sebesar 2% dari pendapatan tahunan, berpotensi menghadapi persoalan serupa dalam hubungan transfer data dengan negara mitra dagang, termasuk Amerika Serikat.

Penulis merekomendasikan agar Indonesia mengadopsi pendekatan yang adaptif dalam reformasi Undang-Undang Perlindungan Data Pribadi (UU PDP). Pendekatan tersebut dilakukan melalui pengadopsian yurisdiksi ekstrateritorial dan prinsip akuntabilitas proaktif sebagaimana diterapkan dalam *General Data Protection Regulation* (GDPR) guna memperkuat perlindungan hak privasi warga negara Indonesia. Dengan demikian, regulasi

nasional diharapkan dapat diberlakukan terhadap perusahaan asing yang memproses data pribadi warga negara Indonesia meskipun beroperasi di luar wilayah yurisdiksi nasional.

Pada saat yang sama, pendekatan *hybrid* tersebut juga perlu mengakomodasi fleksibilitas sektoral sebagaimana diterapkan di Amerika Serikat agar selaras dengan karakteristik otonomi daerah serta kebutuhan pengembangan ekonomi digital nasional yang berkembang secara dinamis. Pendekatan ini penting untuk memastikan bahwa pengaturan perlindungan data pribadi tidak menimbulkan beban yang berlebihan bagi pelaku usaha mikro, kecil, dan menengah (UMKM), maupun sektor-sektor strategis nasional lainnya.

Selain itu, diperlukan penguatan peran Badan Perlindungan Data Pribadi (BPDP) sebagai otoritas pengawas independen yang efektif dan memiliki kewenangan penuh dalam penegakan hukum, pengawasan, serta penyelesaian sengketa di bidang perlindungan data pribadi. Penguatan kelembagaan tersebut bertujuan agar implementasi regulasi tidak hanya bersifat normatif, tetapi juga dapat dilaksanakan secara konsisten, efektif, dan tegas.

Melalui pendekatan yang berlandaskan pada prinsip *accountability*, *proportionality*, dan perlindungan hak asasi manusia, Indonesia diharapkan mampu mewujudkan keseimbangan antara perlindungan privasi yang kuat dengan kebutuhan pertumbuhan ekonomi digital serta kelancaran transfer data lintas batas.

D. Simpulan

Penelitian ini menyimpulkan bahwa terdapat perbedaan mendasar dalam pengaturan normatif hukum perlindungan data pribadi antara Amerika Serikat dan *General Data Protection Regulation* (GDPR) Uni Eropa. Amerika Serikat menerapkan pendekatan sektoral dan fragmentaris yang bergantung pada regulasi di tingkat negara bagian, sedangkan GDPR menganut kerangka regulasi yang komprehensif dengan yurisdiksi ekstrateritorial sebagaimana diatur dalam Pasal 3 serta prinsip akuntabilitas proaktif sebagaimana tercantum dalam Pasal 35. Perbedaan tersebut melahirkan berbagai persoalan hukum berupa konflik norma, kekaburan norma, kekosongan norma, dan tumpang tindih norma akibat fragmentasi regulasi di Amerika Serikat. Permasalahan tersebut berdampak signifikan terhadap mekanisme transfer data lintas batas, khususnya dalam kerangka *EU-US Data Privacy Framework* (DPF). Kerangka tersebut masih dinilai rentan karena fondasi regulasi Amerika Serikat yang tidak seragam belum sepenuhnya memenuhi standar perlindungan yang setara sebagaimana dipersyaratkan dalam GDPR. Kondisi ini menimbulkan ketidakpastian hukum, peningkatan biaya kepatuhan, serta risiko terhadap perlindungan hak privasi subjek data di tengah perkembangan teknologi kecerdasan buatan.

Secara teoritis, penelitian ini menegaskan bahwa pendekatan *market-oriented privacy* yang dianut Amerika Serikat memiliki perbedaan filosofis dengan *rights-based approach* dalam GDPR yang berlandaskan pada perlindungan hak asasi manusia. Pendekatan fragmentaris di Amerika Serikat berpotensi menimbulkan *race to the bottom*, sedangkan GDPR berhasil membentuk standar minimum global (*Brussels Effect*) dalam perlindungan data pribadi.

Bagi Indonesia, temuan penelitian ini menunjukkan urgensi reformasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini merekomendasikan penerapan model *hybrid* yang adaptif melalui integrasi yurisdiksi ekstrateritorial dan prinsip akuntabilitas proaktif dari GDPR guna memperkuat perlindungan hak privasi, dengan tetap mengakomodasi fleksibilitas sektoral sebagaimana diterapkan di Amerika Serikat agar sesuai dengan karakteristik otonomi daerah dan

kebutuhan pengembangan ekonomi digital nasional. Selain itu, penguatan peran Badan Perlindungan Data Pribadi (BPDP) sebagai otoritas independen yang efektif menjadi elemen penting dalam reformasi regulasi tersebut. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi normatif bagi harmonisasi regulasi perlindungan data pribadi di Indonesia dengan standar global, sehingga mampu mendukung kelancaran transfer data lintas batas sekaligus menjamin perlindungan hak privasi masyarakat di era digital.

Daftar Pustaka

Aidun, E. (2025). Data Privacy in the Digital Age: A Comparative Analysis of U.S. and EU Regulations. *University of Cincinnati Law Review*, *93*. https://uclawreview.org/2025/03/05/data-privacy-in-the-digital-age-a-comparative-analysis-of-u-s-and-eu-regulations/

Asmadi, E., Mansar, A., & Eddy, T. (2023). Actualization of Criminal Liability for Personal Data Protection in the Use of Financial Technology: A Comparative Study of Law Number 11 of 2008 Concerning Information and Electronic Transactions and Law Number 27 of 2022 Concerning Protection of Personal Data. *De Lega Lata: Jurnal Ilmu Hukum*, *8*(2). https://doi.org/10.30596/dll.v8i2.15252

Austin. (2025). *2025 Global Threat Report*. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

Buckley, G., Caulfield, T., & Becker, I. (2024). How Might the Gdpr Evolve? A Question of Politics, Pace and Punishment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4830619

Chance, C. (2025). *Data Privacy Legal Trends 2025*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/02/data-privacy-legal-trends-2025.pdf

De Bruin, R. (2022). A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4251540

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

IBM Security. (2025). *Cost of A Data Breach Report 2025*. https://www.ibm.com/reports/data-breach

Jain, A. (2025). AI and Privacy 2024 to 2025: Embracing the Future of Global Legal Developments. *cloudsecurityalliance.org*. https://cloudsecurityalliance.org/blog/2025/04/22/ai-and-privacy-2024-to-2025-embracing-the-future-of-global-legal-developments

Khan, M. N. I. (2025). Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices. *American Journal of Scholarly Research and Innovation*, *04*(01), 138–174. https://doi.org/10.63125/a4gbeb22

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1), 5536763. https://doi.org/10.1049/ise2/5536763

Martono, Akbar, M. G. G., & Rahmatiar, Y. (2025). Law Enforcement of Transnational Cybercrime: Case Study in Indonesia. *De Lega Lata: Jurnal Ilmu Hukum*, *10*(2). https://jurnal.umsu.ac.id/index.php/delegalata/article/view/24627

Prastyanti, R. A., Rahayu, I., Yafi, E., Wardiono, K., & Budiono, A. (2022). Law and Personal Data: Offering Strategies for Consumer Protection in New Normal Situation in Indonesia. *Jurnal Jurisprudence*, *11*(1), 82–99. https://doi.org/10.23917/jurisprudence.v11i1.14756

Samin, H. H., Ismail, D. E., & Rahim, E. I. (2024). The Urgency of Legal Protection of Personal Data. *De Lega Lata: Jurnal Ilmu Hukum*, *9*(2). https://jurnal.umsu.ac.id:444/index.php/delegalata/article/view/19768

Skillcast. (2025). *Biggest GDPR Fines of 2026*. https://www.skillcast.com/blog/biggest-gdpr-fines-2026

Stanford Human-Centered AI. (2025). *AI Index Report 2025*. https://hai-production.s3.amazonaws.com/files/hai_ai_index_report_2025.pdf

Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). Legal Protection of Cybercrime Crimes From Ransomware Attacks and Evaluation of The Cyber Security and Resilience Bill 2025 in Indonesia'S Defense. *De Lega Lata: Jurnal Ilmu Hukum*, *10*(2). https://jurnal.umsu.ac.id:444/index.php/delegalata/article/view/25786

Tschider, C., Compagnucci, M. C., & Minssen, T. (2024). The New EU–US Data Protection Framework's Implications for Healthcare. *Journal of Law and the Biosciences*, *11*(2), lsae022. https://doi.org/10.1093/jlb/lsae022

Wilson, J. M. (2022). Cross-Border Data Transfers: A Balancing Act Through Federal Law. *The Business, Entrepreneurship & Tax Law Review*, *6*(2). https://scholarship.law.missouri.edu/betr/vol6/iss2/10/