**Jurnal Riset Multidisiplin Edukasi**
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 895-914

# KOMPARASI REGULASI PERLINDUNGAN DATA PRIBADI DI UNI EROPA DAN AMERIKA SERIKAT

Royan Hanapi[1], Owen Hutagalung[2], Widi Susanto[3], Indah Dewi Megasari[4]
Magister Hukum, Universitas Islam Kalimantan Muhammad Arsyad Al- Banjari [1,2,3,4]
Email: royanhanapi18@gmail.com[1], hutagalungowen@gmail.com[2], widisusanto27@gmail.com[3]

**Informasi**

Volume : 2
Nomor : 12
Bulan : Desember
Tahun : 2025
E-ISSN : 3062-9624

**Abstract**

*This article presents a comprehensive comparison between the personal data protection regulatory frameworks of the European Union and the United States. The European Union adopts a comprehensive, rights-based approach through the General Data Protection Regulation (GDPR), emphasizing transparency, accountability, and individual control over personal data. In contrast, the United States employs a hybrid model that combines sector-specific federal regulations with state-level privacy laws such as the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), resulting in varying levels of protection across sectors and jurisdictions. This article examines key dimensions of both systems, including scope and extraterritorial reach, legal bases for data processing, data subject rights, obligations of data controllers, enforcement mechanisms, and the nature of sanctions. It also explores each system's approach to cross-border data transfers and analyzes practical implications for global businesses, regulatory bodies, and individuals as data subjects. The findings indicate that the GDPR provides more stringent and harmonized safeguards, whereas the U.S. system offers greater flexibility but remains fragmented. The article concludes by highlighting the strengths and weaknesses of both regulatory models and offering policy recommendations aimed at strengthening data protection while supporting technological advancement and economic innovation in the digital era.*

***Keyword:*** *GDPR, CCPA, CPRA, privacy, data protection*

***Abstrak***

*Artikel ini membahas perbandingan komprehensif antara rezim regulasi perlindungan data pribadi di Uni Eropa dan Amerika Serikat. Uni Eropa menerapkan kerangka perlindungan data yang bersifat komprehensif dan berbasis hak melalui General Data Protection Regulation (GDPR), yang menekankan prinsip transparansi, akuntabilitas, dan kontrol individu atas data pribadi mereka. Sebaliknya, Amerika Serikat menggunakan pendekatan campuran yang menggabungkan peraturan federal sektoral dengan undang-undang privasi tingkat negara bagian, seperti California Consumer Privacy Act (CCPA) dan California Privacy Rights Act (CPRA), yang memberikan perlindungan berbeda berdasarkan sektor dan yurisdiksi. Artikel ini menganalisis berbagai aspek utama kedua sistem, termasuk ruang lingkup dan penerapan ekstrateritorial, dasar hukum pemrosesan data, hak subjek data, kewajiban pengendali data, mekanisme penegakan, dan jenis sanksi. Selain itu, pembahasan mencakup pendekatan masing-masing terhadap transfer data lintas batas, serta implikasi praktisnya bagi pelaku usaha global, badan pengawas, dan individu sebagai pemilik data. Temuan dalam kajian ini menunjukkan bahwa GDPR menawarkan perlindungan lebih ketat dan seragam, sementara sistem Amerika Serikat cenderung lebih fleksibel namun fragmentatif. Artikel ini menyimpulkan dengan menyoroti kelebihan dan kekurangan masing-masing model serta memberikan rekomendasi kebijakan yang bertujuan untuk memperkuat perlindungan data sambil tetap mendukung pengembangan*

*teknologi dan inovasi ekonomi di era digital*

***Kata Kunci:*** *GDPR, CCPA, CPRA, privasi, perlindungan data*

## A. PENDAHULUAN

Terutama seiring pertumbuhan ekonomi digital dan ketergantungan global pada teknologi informasi, perlindungan data pribadi telah menjadi topik yang semakin penting dalam perdebatan internasional tentang tata kelola digital. Data pribadi telah berkembang menjadi komoditas strategis yang mendorong inovasi ekonomi, strategi pemasaran, personalisasi layanan, dan kecerdasan buatan serta sistem analitik canggih di ekosistem digital kontemporer. Tidak lagi sekadar produk dari aktivitas digital.[1] Data dianggap sebagai "minyak baru" bagi perekonomian global, dan berfungsi sebagai dasar untuk pengambilan keputusan dan kemajuan dalam berbagai teknologi lintas sektor, seperti perbankan, kesehatan, pemerintahan, dan hiburan digital. Namun, peningkatan nilai data ini juga diikuti oleh risiko penyalahgunaan, pelacakan yang berbahaya, pelanggaran privasi, dan ancaman keamanan siber. Kebocoran data berskala besar, seperti yang terjadi pada Cambridge Analytica dan perusahaan teknologi global, menunjukkan betapa lemahnya perlindungan data dapat memiliki konsekuensi sosial, politik, dan ekonomi yang signifikan. Dalam situasi seperti ini, menjaga data pribadi sangat penting untuk memastikan kemajuan teknologi sejalan dengan perlindungan hak asasi manusia, terutama hak atas privasi dan keamanan informasi. Oleh karena itu, pembuat kebijakan, akademisi, dan pelaku industri di seluruh dunia telah berkonsentrasi pada masalah privasi, transparansi pengelolaan data, dan kerangka hukum yang melindungi informasi pribadi. Dalam situasi seperti ini, membuat kebijakan perlindungan data bukan hanya masalah teknis hukum; itu juga merupakan masalah etika sosial, kedaulatan data, dan keseimbangan antara perlindungan individu dalam ekosistem digital yang terus berkembang dengan keuntungan ekonomi.

Melalui penerapan Regulasi Perlindungan Data Umum (GDPR), yang ditetapkan pada tahun 2018, Uni Eropa menjadi pemimpin dalam perlindungan data pribadi. GDPR dianggap sebagai standar internasional untuk peraturan privasi. GDPR menggunakan pendekatan berbasis hak, yang menegaskan bahwa orang harus dilindungi selama proses pengolahan data.[2] Metode ini berakar pada gagasan bahwa hukum supranasional Uni Eropa melindungi

[1] Dhani Gunawan Idat, "Memanfaatkan Era Ekonomi Digital Untuk Memperkuat Ketahanan Nasional," *Jurnal Lemhannas RI* 7, no. 2 (2019): 5–11, https://doi.org/10.55960/jlri.v7i2.67.

[2] Gracella Leonora dan Roy Vincentius Pratikno, "REGULASI PERDAGANGAN TERKAIT PERLINDUNGAN PRIVASI KONSUMEN DALAM EKSPANSI BISNIS DI UNI EROPA: STUDI KASUS ALIBABA," *Verity: Jurnal Ilmiah Hubungan*

hak privasi, seperti yang dinyatakan dalam Charter of Fundamental Rights of the European Union. GDPR menetapkan prinsip-prinsip dasar seperti integritas dan kerahasiaan data, legalitas, transparansi, tujuan khusus, minimisasi data, akurasi, dan batasan penyimpanan. GDPR mewajibkan organisasi untuk menerapkan pendekatan "privacy by design and by default"—memasukkan perlindungan privasi sejak tahap perancangan sistem dan proses. Uni Eropa berkomitmen untuk memberikan kontrol total atas informasi pribadi orang-orang melalui persyaratan yang ketat mengenai hak akses, hak untuk dilupakan, hak portabilitas data, dan pembatasan pemrosesan. Selain itu, GDPR menetapkan mekanisme penegakan yang kuat melalui otoritas perlindungan data (DPAs) di setiap negara anggota. Sanksi administratif dapat mencapai hingga 4% dari pendapatan perusahaan di seluruh dunia.[3] Oleh karena itu, pendekatan Uni Eropa tidak hanya menetapkan standar hukum yang jelas dan konsisten, tetapi juga menunjukkan nilai dan visi politik bahwa kemajuan teknologi harus seiring dengan perlindungan hak manusia sebagai pemilik data.

Amerika Serikat menggunakan pendekatan perlindungan data yang pragmatis, terfragmentasi, dan berfokus pada sektor dan kepentingan pasar, berbeda dengan Uni Eropa. Kerangka hukum sektoral seperti Health Insurance Portability and Accountability Act (HIPAA) untuk bidang kesehatan, Gramm-Leach-Bliley Act (GLBA) untuk bidang keuangan, dan Children's Online Privacy Protection Act (COPPA) untuk bidang data anak menjalankan sistem undang-undang privasi Amerika Serikat tanpa undang-undang federal yang komprehensif. Selain itu, pengawasan yang lebih luas diperkuat oleh tugas Federal Trade Commission (FTC) untuk menghentikan praktik bisnis yang menyesatkan atau merugikan konsumen. undang-undang privasi negara bagian baru-baru ini, seperti California Consumer Privacy Act (CCPA) dan California Privacy Rights Act (CPRA), lebih mendekati prinsip perlindungan komprehensif yang ditawarkan oleh GDPR. Meskipun demikian, perbedaan aturan di antara negara menyebabkan standar kepatuhan yang berbeda, yang menghalangi bisnis internasional. Metode ini mencerminkan prinsip ekonomi dan kebijakan utama Amerika yang menekankan pertumbuhan industri teknologi, kebebasan pasar, dan inovasi sebagai motor ekonomi nasional. Amerika Serikat mengutamakan fleksibilitas, yang memungkinkan industri untuk berkembang tanpa dibatasi oleh kerangka kepatuhan yang

---

*Internasional (International Relations Journal)* 16, no. 32 (2024): 25–43, europe, https://doi.org/10.19166/verity.v16i32.9101.

[3] Azza Fitrahul Faizah dkk., "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 1, no. 3 (2023): 01–27, https://doi.org/10.51903/hakim.v1i3.1222.

terlalu ketat. Namun, banyak kritik terhadap sistem ini karena kurangnya perlindungan konsumen dan kurangnya integrasi hak privasi individu. Ini terutama terjadi di tengah meningkatnya kekhawatiran publik tentang penyalahgunaan data oleh perusahaan dan lembaga pemerintah.

Disebabkan perbedaan mendasar antara sistem hukum UE dan AS, ada konsekuensi yang signifikan bagi tata kelola data di seluruh dunia. Ini terutama berlaku untuk perusahaan multinasional, regulator, dan pengguna layanan digital di seluruh dunia. Perusahaan internasional yang beroperasi di kedua yurisdiksi harus membuat rencana kepatuhan yang canggih untuk memenuhi persyaratan ketat GDPR sekaligus menyesuaikan diri dengan mekanisme yang fleksibel di bawah kerangka hukum Amerika yang rumit. Ini biasanya membutuhkan investasi besar dalam infrastruktur kepatuhan, audit internal, pelatihan SDM, dan dokumentasi pemrosesan data. Selain itu, salah satu masalah terbesar dalam hubungan transatlantik adalah masalah transfer data lintas batas, terutama setelah Mahkamah Uni Eropa membatalkan Privacy Shield dan munculnya perdebatan lama tentang pengawasan pemerintah AS terhadap data digital. Di tingkat publik, ketidaksetaraan perlindungan privasi antarwilayah muncul karena perbedaan tingkat perlindungan yang berbeda berdampak pada kepercayaan pengguna terhadap layanan digital. Perbandingan ini memberi pembuat kebijakan kesempatan untuk berbicara tentang cara terbaik untuk menyeimbangkan kebutuhan untuk inovasi digital, keamanan negara, dan perlindungan hak individu. Harmonisasi kebijakan dan kerja sama internasional menjadi semakin penting di tengah perkembangan kecerdasan buatan, penggunaan big data di sektor publik dan swasta, dan meningkatnya ancaman kejahatan siber. Oleh karena itu, pemahaman mendalam tentang kedua model regulasi ini sangat penting untuk pengembangan kebijakan masa depan yang berkelanjutan dan responsif terhadap perkembangan teknologi yang cepat.

## B. METODE PENELITIAN

Penelitian ini menggunakan metodologi kualitatif dan berfokus pada analisis sistematis instrumen hukum, pedoman regulasi, literatur akademik, dan publikasi kebijakan publik yang berkaitan dengan perlindungan data pribadi.[4] Metode ini dipilih karena penelitian ini berfokus pada perbandingan kerangka hukum dan interpretasi perlindungan data di Uni Eropa dan AS. Oleh karena itu, penelitian ini tidak hanya bertujuan untuk menemukan perbedaan dalam peraturan di kedua yurisdiksi tersebut, tetapi juga untuk memahami

[4] Elia Ardyan dkk., *METODE PENELITIAN KUALITATIF DAN KUANTITATIF : Pendekatan Metode Kualitatif dan Kuantitatif di Berbagai Bidang* (PT. Sonpedia Publishing Indonesia, 2023).

konsekuensi praktis dari penerapan setiap sistem peraturan dalam konteks tata kelola data global.

Proses analisis bergantung pada sumber hukum primer. Untuk wilayah Uni Eropa, perhatian utama dberikan pada Peraturan Perlindungan Data Umum (GDPR) dan pedoman interpretasi yang diterbitkan oleh Dewan Perlindungan Data Eropa (EDPB), Komisi Eropa, dan otoritas perlindungan data di negara anggota. Dokumen ini memastikan pemahaman yang tepat tentang terminologi, prinsip substantif, yurisdiksi, dan prosedur implementasi dan penegakan. Selain itu, analisis kerangka hukum sektoral federal seperti Federal Trade Commission Act, Health Insurance Portability and Accountability Act (HIPAA), dan Children's Online Privacy Protection Act (COPPA) digunakan untuk melakukan penelitian undang-undang negara bagian tentang privasi, terutama California Consumer Privacy Act (CCPA) dan California Privacy Rights Act (CPRA). Dengan menggunakan kombinasi ini, penelitian dapat mengidentifikasi ciri-ciri yang membedakan regulasi privasi di Amerika Serikat, serta kecenderungan perubahan pengaturan yang dipengaruhi oleh perkembangan digital dan tekanan publik.

Penelitian ini menggunakan sumber sekunder selain sumber hukum primer untuk memperkuat kerangka teoritis dan memberikan perspektif analitis yang lebih luas. Sumber-sumber ini termasuk buku, artikel jurnal ilmiah, white papers, dan publikasi think tank dan lembaga penelitian yang berfokus pada kebijakan data dan hukum teknologi. Laporan pembaruan regulasi dan publikasi media yang dapat diandalkan juga digunakan sebagai sumber pendukung untuk mengetahui perkembangan terbaru yang belum sepenuhnya didokumentasikan dalam literatur akademik. Sangat penting untuk memiliki sumber sekunder ini untuk memastikan bahwa analisis tidak hanya bersifat normatif tetapi juga mencerminkan praktik implementasi dan perubahan politik hukum terkait perlindungan data pribadi.

Secara keseluruhan, pendekatan penelitian ini menggabungkan sumber primer untuk validitas konseptual dan hukum, dan sumber sekunder digunakan untuk analitis dan konteks akademik. Untuk menjamin kebenaran ilmiah dan kemudahan verifikasi bagi pembaca dan peneliti berikutnya, daftar pustaka akan mencantumkan semua rujukan yang digunakan dalam penelitian ini secara sistematis dan lengkap.

**3. Kerangka Regulasi Uni Eropa (GDPR)**

General Data Protection Regulation (GDPR), yang resmi berlaku pada tanggal 25 Mei 2018, adalah undang-undang penting dalam perlindungan data di seluruh dunia. Tujuan dari

undang-undang ini adalah untuk menggantikan Directive 95/46/EC dan menciptakan standar perlindungan data yang lebih kuat, konsisten, dan tersebar di seluruh Uni Eropa. GDPR dirancang untuk menjadi alat hukum yang langsung berlaku tanpa memerlukan pelaksanaan undang-undang nasional, sehingga memastikan kebijakan privasi di seluruh wilayah bekerja sama serta mengurangi kekacauan hukum sebelumnya dalam kerangka Data Protection Directive. Sebagaimana ditegaskan dalam Charter of Fundamental Rights of the European Union, khususnya Pasal 7 dan 8, penerapan GDPR menunjukkan komitmen Uni Eropa untuk menjadikan perlindungan data pribadi sebagai bagian penting dari hak asasi manusia.

GDPR mengatur beberapa prinsip dasar pemrosesan data pribadi yang menjadi tanggung jawab utama baik pengendali data maupun pemroses data. Salah satu prinsip yang digunakan dalam pemrosesan data adalah legalitas, keadilan, dan transparansi. Ini berarti bahwa data hanya boleh digunakan untuk tujuan yang jelas dan diperlukan; mengurangi data untuk memastikan hanya informasi yang relevan dan diperlukan yang dikumpulkan; dan memastikan bahwa data yang diproses benar dan akurat sesuai kebutuhan. GDPR mewajibkan pengendali untuk tidak menyimpan data lebih lama dari yang diperlukan. Selain itu, prinsip integritas dan kerahasiaan menekankan betapa pentingnya mengambil tindakan keamanan organisasi dan teknis untuk mencegah akses tidak sah, kehilangan, atau kerusakan data pribadi. Pada akhirnya, prinsip akuntabilitas menuntut bahwa pengendali data tidak hanya mematuhi peraturan GDPR tetapi juga dapat membuktikan kepatuhan mereka melalui dokumentasi, prosedur internal, dan sistem audit.

GDPR tidak hanya menetapkan dasar, tetapi juga memberi orang hak yang luas sebagai subjek data. Di antara hak-hak ini adalah hak untuk mengakses data pribadi yang telah diproses, hak untuk melakukan koreksi terhadap data yang salah, dan hak untuk meminta penghapusan data dalam situasi tertentu, yang juga dikenal sebagai hak untuk lupa.[5] Selain itu, setiap orang memiliki hak untuk membatasi jumlah data yang diproses, hak atas portabilitas data, yang memungkinkan data ditransfer antar layanan dengan mudah, dan hak untuk menolak pemrosesan yang didasarkan pada kepentingan publik atau alasan sah pengendali data. Salah satu tujuan dari hak-hak ini adalah untuk memberi orang lebih banyak kebebasan untuk mengontrol informasi pribadi mereka sendiri. Mereka juga bertujuan untuk menciptakan hubungan antara orang dan entitas pengelola data, baik di sektor publik maupun swasta.

[5] Muhammad Akbar Eka Pradana dan Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative: Journal Of Social Science Research* 4, no. 4 (2024): 3412–25, https://doi.org/10.31004/innovative.v4i4.13476.

Selain itu, GDPR memberikan struktur kelembagaan penegakan yang kuat melalui otoritas perlindungan data nasional, yang dikenal sebagai Data Protection Authorities. Otoritas ini memiliki otoritas untuk melakukan investigasi, memberikan peringatan dan perintah, serta menjatuhkan sanksi administratif. Di tingkat regional, European Data Protection Board (EDPB) bertanggung jawab untuk memastikan bahwa GDPR diterapkan secara konsisten di semua negara anggota melalui pedoman, pendapat, dan mekanisme penyelesaian sengketa lintas yurisdiksi. Rezim penegakan ini diperkuat dengan ancaman sanksi administratif yang berat. Pelanggaran serius dapat dikenai denda hingga €20 juta, atau 4% dari pendapatan global setiap tahun, atau lebih tinggi. Hal ini menunjukkan sikap tegas Uni Eropa dalam menjamin kepatuhan dan menumbuhkan budaya perlindungan data sebagai bagian dari manajemen perusahaan kontemporer.

GDPR menjadi standar untuk perlindungan data pribadi di seluruh dunia dengan struktur hukum yang rinci, berbasis hak, dan mekanisme penegakan yang kuat. Prinsip-prinsip GDPR telah menjadi model tata kelola data internasional di era ekonomi digital, dan banyak negara di luar Eropa telah mengadopsi atau mengubah undang-undang mereka untuk mengikutinya.[6]

Fakta penting tentang ekstrateritorialitas GDPR mencakup banyak hal—ia berlaku untuk organisasi yang berbasis di UE dan organisasi luar-UE yang menawarkan barang dan jasa kepada orang di UE atau memantau perilaku mereka. Ini berarti bahwa bisnis di seluruh dunia harus mematuhi GDPR ketika menargetkan pasar UE. Namun, otoritas UE sedang memperhatikan masalah penegakan praktis saat menerapkannya pada entitas luar-UE. edpb.europa.eu+1

**4. Kerangka Regulasi Amerika Serikat**

Sampai tahun 2025, Amerika Serikat belum memiliki undang-undang privasi federal yang komprehensif dan luas, berbeda dengan Uni Eropa, yang menerapkan peraturan perlindungan data yang berbasis hak. Alih-alih, sistem hukum privasi AS berkembang melalui pendekatan case-by-case dan undang-undang federal khusus sektor, pedoman lembaga pengawas, dan peraturan negara bagian. Struktur ini mencerminkan filosofi hukum Amerika yang lebih pragmatis dan berorientasi pasar, di mana intervensi pemerintah cenderung dilakukan hanya ketika terdapat risiko besar bagi konsumen atau sektor tertentu daripada melalui regulasi universal yang bersifat ex ante.

[6] Yacinta Tira Varany dan Listyowati Sumanto, "Dinamika Sistem Hukum Pelindungan Data Pribadi: Analisis Interaksi Struktur, Substansi, Dan Kultur Hukum Di Era Big Data," *Jurnal Impresi Indonesia* 4, no. 11 (2025): 5172–85, https://doi.org/10.58344/jii.v4i11.7182.

Pada tingkat federal, ada undang-undang sektoral yang mengatur perlindungan data pribadi dengan standar kepatuhan yang berbeda untuk bidang tertentu. HIPAA (Health Insurance Portability and Accountability Act) mengatur rekam medis dan data kesehatan; Gramm-Leach-Bliley Act (GLBA) mengatur standar privasi data sektor keuangan; Fair Credit Reporting Act (FCRA) mengatur pelaporan kredit konsumen; dan Children's Online Privacy Protection Act (COPPA) melindungi data anak di bawah 13 tahun saat menggunakan layanan online. Selain itu, kewajiban lembaga pengelola data, terutama di bidang telekomunikasi, pendidikan, dan energi, diperkuat oleh peraturan dan pedoman tambahan yang dikeluarkan oleh lembaga federal. Meskipun begitu, tidak ada persetujuan sektoral yang menyeluruh, sehingga setiap industri memiliki kebutuhan privasi yang berbeda.

Federal Trade Commission (FTC) adalah lembaga utama yang bertanggung jawab untuk melakukan pengawasan federal terhadap praktik bisnis yang dianggap menipu atau merugikan konsumen. Memanfaatkan kewenangan ini, FTC bertindak sebagai regulator utama untuk menegakkan standar privasi dan keamanan data. Namun, lingkupnya berbeda dari kerangka hak privasi yang jelas di Eropa. Selain FTC, Komisi Komunikasi Federal (FCC) dan lembaga di sektor keuangan dan kesehatan juga melakukan pengawasan di yurisdiksi mereka sendiri. Peran lembaga-lembaga ini menunjukkan bahwa sistem AS bergantung pada kepatuhan sektoral dan perlindungan konsumen daripada standar hak privasi individu.[7]

Tidak ada peraturan federal yang lengkap, banyak negara bagian mulai mengesahkan undang-undang privasi komprehensif sebagai tanggapan terhadap meningkatnya kekhawatiran publik tentang penyalahgunaan data digital, terutama setelah skandal Cambridge Analytica. Dengan mengadopsi California Consumer Privacy Act (CCPA) pada 2018 dan diperkuat oleh California Privacy Rights Act (CPRA) pada 2020, California menjadi pemimpin dengan memperluas perlindungan privasi konsumen dan membentuk Agen Perlindungan Privasi California (CPPA) sebagai badan penegak independen. Negara bagian lain, seperti Virginia, Colorado, Connecticut, dan Utah, kemudian mengadopsi kerangka privasi serupa, tetapi dengan persyaratan dan cakupan yang berbeda. Di tengah tren ini, ada "patchwork" undang-undang negara bagian yang semakin kompleks yang mengharuskan perusahaan mematuhi standar privasi yang berbeda tergantung pada lokasi bisnis mereka dan jenis data yang mereka proses.

[7] Nurul Mubarikah, "KEWAJIBAN ENDORSER ATAS PENGANJURAN SUATU PRODUK PADA MEDIA SOSIAL MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA DALAM PERBANDINGAN DENGAN AMERIKA SERIKAT, INGGRIS DAN INDIA," *"Dharmasisya" Jurnal Program Magister Hukum FHUI* 1, no. 1 (2021), https://scholarhub.ui.ac.id/dharmasisya/vol1/iss1/13.

Kongres Amerika Serikat terus bekerja untuk membuat undang-undang privasi federal yang lengkap. American Data Privacy and Protection Act (ADPPA), salah satu undang-undang yang paling terkenal, bertujuan untuk menetapkan standar minimum nasional sekaligus membatasi pengumpulan data, memperkuat hak pengguna, dan meningkatkan otoritas FTC. Hingga saat ini, belum ada kesepakatan politik terakhir. Ini terutama karena perdebatan tentang preemption federal (apakah hukum federal akan menggantikan hukum negara bagian seperti CPRA) dan mekanisme hak tindakan privasi yang memungkinkan orang menggugat pelanggaran privasi. Oleh karena itu, sistem undang-undang privasi Amerika Serikat terus berubah dan mungkin mengalami reformasi struktural di masa mendatang. Namun, sistem ini masih diwarnai oleh perbedaan dan perbedaan antar yurisdiksi.

Secara keseluruhan, metode Amerika Serikat lebih kompleks dan tidak konsisten dari sudut pandang perlindungan hak individu, tetapi memberikan kerangka perlindungan data yang lebih fleksibel bagi pelaku industri. Meskipun model ini dianggap mendorong inovasi dan kemajuan ekonomi digital, keterbatasan cakupan dan harmonisasi hukumnya menyebabkan masalah bagi konsumen dan organisasi lintas negara.

## C. HASIL DAN PEMBAHASAN

### 5.1 UE/GDPR

Peraturan dasar untuk hampir semua pemrosesan data pribadi yang dilakukan oleh sektor pemerintah dan swasta di seluruh UE, serta peraturan yang berlaku di luar UE ketika orang ditargetkan atau diawasi. Ini menetapkan tanggal mulai berlakunya GDPR di seluruh dunia. GDPR+

Amerika Serikat: Tidak ada aturan tunggal; yurisdiksi didasarkan pada jenis data, sektor, dan lokasi data. Negara bagian dapat memberlakukan persyaratan terbatas di luar wilayah negara bagian, seperti membangun perusahaan yang melayani warga negara bagian. Kepatuhan nasional dan internasional menjadi sulit karena ketidakpastian ini. IAAP

### 5.2 Dasar Hukum Pemrosesan

GDPR memerlukan dasar hukum jelas (kontrak, persetujuan, kepatutan publik, kepentingan sah, kewajiban hukum, atau perlindungan kepentingan vital). Persetujuan harus tegas, bebas, spesifik, dan informasi. GDPR

Amerika Serikat: Tidak ada dasar hukum yang umum untuk pemrosesan di semua industri; biasanya bergantung pada kontrak, persetujuan pengguna, atau aturan khusus

industri. Meskipun metode ini lebih fleksibel, ia menawarkan perlindungan hak subjektif yang lebih luas.

**5.3 Hak Individu**

GDPR mengatur hak akses, perbaikan, penghapusan, pembatasan, portabilitas, dan keberatan. Hak-hak ini dilindungi oleh otoritas deputi presiden Uni Eropa. GDPR

Amerika Serikat: Undang-undang negara bagian memberikan hak-hak tertentu, seperti akses, penghapusan, dan pembatasan penjualan data di CCPA/CPRA. Namun, hak-hak ini tidak universal. Negara bagian dan sektor memiliki hak yang berbeda.

**5.4 Kewajiban Pengontrol & Pemroses**

Prinsip akuntabilitas dalam GDPR adalah salah satu elemen penting yang membedakan pendekatan Uni Eropa terhadap undang-undang lainnya. GDPR tidak hanya mewajibkan pengendali dan pemroses data (data controller) untuk melakukan hal-hal tertentu, tetapi juga meminta mereka untuk menunjukkan kepatuhan melalui instruksi, prosedur internal, dan mekanisme pengawasan yang terorganisir.[8] Ini ditunjukkan oleh sejumlah kewajiban administratif, seperti memelihara catatan operasi pemrosesan (ROPA), mengembangkan kebijakan dan prosedur perlindungan data internal, dan menerapkan evaluasi dampak perlindungan data (DPIA) untuk proses pemrosesan data yang dinilai berisiko tinggi. Selain itu, GDPR mewajibkan penerapan konsep privacy by design dan privacy by default, yang berarti bahwa organisasi harus memastikan bahwa perlindungan data sudah ada sejak awal. Untuk memastikan pihak ketiga yang terlibat dalam pemrosesan data memenuhi standar perlindungan yang sama, kontrak dengan pemroses data juga diatur secara ketat. Dalam kerangka ini, GDPR mendorong budaya manajemen risiko dan tata kelola privasi yang proaktif dan berkelanjutan.

Sebaliknya, peraturan di Amerika Serikat lebih terorganisir dalam hal akuntabilitas data. Meskipun tidak ada undang-undang nasional yang lengkap yang mewajibkan perusahaan untuk mengikuti standar akuntabilitas yang sama, undang-undang sektoral dan negara bagian tertentu mengatur tata kelola privasi. HIPAA, misalnya, menetapkan bahwa entitas yang tunduk pada regulasi kesehatan harus menerapkan kebijakan, prosedur administratif, dan langkah-langkah teknis dan fisik yang memadai untuk menjaga kerahasiaan dan integritas data kesehatan. Selain itu, California Privacy Rights Act (CPRA) menetapkan audit privasi rutin, penilaian risiko, dan perjanjian dengan vendor dan penyedia layanan untuk

[8] Qurratul Hilma, "INTEGRASI GENERAL DATA PROTECTION REGULATION DALAM REGULASI PRIVASI DATA: SOLUSI TANTANGAN TEKNOLOGI KECERDASAN BUATAN," *Jurnal Legislatif*, 9 Oktober 2025, 95–112, https://doi.org/10.20956/jl.v8i2.44141.

memastikan praktik pengelolaan data pihak ketiga memenuhi standar perlindungan privasi konsumen. Meskipun demikian, kurangnya peraturan privasi federal yang komprehensif menyebabkan yurisdiksi dan sektor di Amerika Serikat melakukannya dengan cara yang berbeda.

**5.5 Penegakan & Sanksi**

Rezim penegakan hukum yang diatur oleh Regulasi Perlindungan Data Umum Uni Eropa (General Data Protection Regulation, atau GDPR) dirancang untuk bersifat kuat, terorganisir, dan memberikan hukuman yang keras bagi mereka yang melanggar. GDPR memberikan otoritas perlindungan data nasional kewenangan besar untuk melakukan investigasi, audit, dan penegakan hukum terhadap organisasi yang terbukti melanggar peraturan perlindungan data.[9] GDPR menetapkan denda administratif yang sangat besar, mencapai hingga €20 juta, atau 4% dari pendapatan tahunan global perusahaan. Ini menunjukkan bahwa Uni Eropa memprioritaskan penegakan privasi, terutama dalam hal perusahaan multinasional yang kuat. GDPR memungkinkan sanksi non-finansial, seperti pembatasan sementara atau permanen terhadap operasi pemrosesan data, penghentian pengiriman data lintas negara, atau kewajiban untuk melakukan perubahan struktural dalam proses pengelolaan data. Selain itu, mekanisme koordinasi antarnegara yang dikelola oleh European Data Protection Board (EDPB) memastikan bahwa pelaksanaan penegakan hukum selaras antara yurisdiksi di seluruh Uni Eropa, termasuk penerapan sistem satu pintu untuk kasus lintas negara. Metode ini meningkatkan konsistensi regulator dan meningkatkan prediktabilitas entitas bisnis tentang kepatuhan yang harus dipenuhi.

Sebaliknya, rezim penegakan privasi di Amerika Serikat lebih terpisah dan terpisah berdasarkan struktur hukum negara yang mengandalkan peraturan khusus dan otoritas penegakan yang tersebar di berbagai sektor. Tidak ada undang-undang federal yang komprehensif tentang perlindungan data. Namun, lembaga seperti Federal Trade Commission (FTC) bertanggung jawab atas praktik bisnis yang curang atau tidak adil, termasuk pengelolaan data pribadi. Tidak seperti denda otomatis berskala besar seperti yang diatur oleh GDPR, sanksi di yurisdiksi federal biasanya bergantung pada persetujuan keputusan, penyelesaian hukum jangka panjang, atau kewajiban untuk memperbaiki praktik privasi perusahaan. Sebaliknya, undang-undang negara bagian seperti California Privacy Rights Act (CPRA) memberikan otoritas tambahan untuk menerapkan denda finansial dan tindakan

[9] Dzikrina Laili Kusumadewi dan Akhmad Cahyono, "Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa (General Data Protection Regulation)," *Lex Patrimonium* 2, no. 2 (2023), https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/12.

penegakan tambahan terhadap pelanggaran privasi. Namun, sanksi, terutama yang berkaitan dengan persentase pendapatan global perusahaan, masih kurang besar dan tidak sebanding dengan wewenang yang diberikan oleh GDPR.

Oleh karena itu, membandingkan kedua sistem menunjukkan bahwa filosofi dan struktur kelembagaan yang berbeda dalam penegakan hukum privasi berbeda. Sementara Amerika Serikat menggunakan model penegakan sektor-spesifik dan berbasis yurisdiksi campuran antara negara bagian dan federal, Uni Eropa menggunakan pendekatan yang sangat terpusat, sistematik, dan berorientasi hukuman terhadap pelanggaran. Perbedaan ini sangat penting bagi perusahaan global karena mereka harus mengubah strategi kepatuhan lintas yurisdiksi. Ini terutama penting karena risiko finansial dan reputasi di wilayah UE jauh lebih besar dibandingkan dengan sistem penegakan di Amerika Serikat.

### 5.6 Transfer Data Lintas Batas

Transfer data lintas batas negara adalah masalah penting dalam rezim perlindungan data UE karena mengatur bagaimana data pribadi warga UE dapat dipindahkan dan diproses di luar UE. GDPR menetapkan aturan ketat untuk transfer data internasional untuk memastikan bahwa perlindungan data orang tetap sama meskipun data mereka keluar dari yurisdiksi UE. Tidak ada dasar hukum yang sah yang membenarkan transfer data.[10] Contoh dasar hukum yang sah termasuk keputusan kecukupan yang dikeluarkan oleh Komisi Eropa, penerapan mekanisme perlindungan standar seperti Klausul Kontrak Standar (SCC), atau penerapan instrumen kebijakan internal perusahaan seperti Klausul Perusahaan Terikat (BCR). Selain itu, GDPR memasukkan metode yang menekankan penilaian risiko dan penerapan langkah pengamanan tambahan, terutama setelah keputusan penting dari Court of Justice of the European Union (CJEU) dalam kasus Schrems II yang membatalkan Perlindungan Privasi Uni Eropa-Amerika Serikat. UE mengkhawatirkan potensi akses pemerintah asing terhadap data pribadi, terutama terkait program pengawasan intelijen AS. Akibatnya, perusahaan yang mentransfer data sekarang diharuskan untuk meninjau rezim hukum negara tujuan secara menyeluruh untuk memastikan bahwa mereka memiliki perlindungan yang memadai. Akibatnya, ini meningkatkan kesulitan kepatuhan dan biaya operasional bagi perusahaan multinasional. Berbicara lebih lanjut tentang standar teknis dan hukum, seperti diskusi tentang Framework Data Privacy EU-US sebagai pengganti Privacy

[10] Fanisa Mayda Ayiliani dan Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–55, https://doi.org/10.14710/jphi.v6i3.%p.

Shield, menunjukkan betapa berubahnya peraturan transfer data internasional di bawah GDPR.

Sementara itu, ada banyak perbedaan dalam cara hukum Amerika Serikat menangani transfer data internasional. Amerika Serikat tidak memiliki alat federal yang mendefinisikan dan melindungi transfer data lintas batas. Tidak ada hukum nasional yang melindungi data warga negara asing yang diproses di Amerika Serikat, karena hukum privasi sektoral dan tidak terpusat membuat AS bergantung pada kebijakan internal perusahaan dan kontrak komersial untuk mengatur transfer data. Perusahaan AS yang beroperasi atau memberikan layanan di wilayah Uni Eropa harus mematuhi GDPR melalui mekanisme seperti SCC. Hal ini memaksa perusahaan AS untuk mengadopsi kepatuhan di luar wilayah negara tersebut. Namun, ketidakpastian hukum yang disebabkan oleh perubahan regulasi dan kemungkinan pengawasan pemerintah AS terhadap data digital menambah masalah ini. Metode berbasis kontrak tanpa pengakuan undang-undang privasi federal yang menyeluruh menciptakan lingkungan yang tidak seragam dan menuntut perusahaan untuk membuat strategi mitigasi risiko yang lebih kompleks untuk memenuhi permintaan pasar di seluruh dunia, terutama di UE, yang memiliki peraturan perlindungan data yang lebih ketat.

Oleh karena itu, melihat kerangka transfer data lintas batas yang digunakan UE dan AS menunjukkan perbedaan filosofis dan institusional yang signifikan. Uni Eropa menetapkan perlindungan data sebagai hak utama dan membuat dasar untuk menjaga tingkat perlindungan yang sama di seluruh dunia. Namun, bisnis yang ingin tetap beroperasi di seluruh dunia harus menavigasi berbagai mekanisme kepatuhan eksternal, terutama yang berkaitan dengan pemrosesan data warga UE, karena Amerika Serikat mengadopsi pendekatan yang lebih terdesentralisasi dan berbasis praktik pasar. Perbedaan ini menunjukkan masalah kebijakan dan hukum, serta strategi bisnis, investasi teknologi, dan standar tata kelola data internasional.

**6. Studi Kasus**

Penggunaan GDPR di Uni Eropa: Sejak diberlakukan, GDPR telah menjadi salah satu undang-undang penegakan hukum yang paling aktif untuk melindungi hak privasi warga. Banyak kasus penting menunjukkan komitmen otoritas Eropa terhadap perlindungan hak privasi warga. Misalnya, pada tahun 2021, otoritas perlindungan data Luksemburg denda Amazon sebesar €746 juta karena gagal mendapatkan persetujuan yang sah untuk personalisasi iklan berbasis data pengguna. Ini adalah denda terbesar yang pernah diberikan oleh GDPR. Kasus lain melibatkan Meta (Facebook/Instagram/WhatsApp), yang berulang kali

didenda miliaran euro oleh lembaga penegakan hukum karena praktik pengolahan data, ketidaktransparanan mekanisme persetujuan, dan pelanggaran terkait transfer data ke Amerika Serikat. Selain itu, Google menghadapi sejumlah tindakan korektif dan denda, salah satunya adalah denda €50 juta oleh otoritas Prancis (CNIL) atas pelanggaran transparansi dan validitas persetujuan dalam personalisasi layanan periklanan.

Beberapa negara Eropa melarang pemrosesan dan denda perusahaan teknologi besar seperti Clearview AI karena mengumpulkan data biometrik dari internet tanpa persetujuan subjek data. Kasus-kasus tersebut menunjukkan bahwa GDPR berlaku untuk perusahaan di Eropa dan di luar negeri. Pembuat undang-undang ini mengikuti prinsip-prinsip GDPR, yang menempatkan privasi sebagai hak utama dan menerapkan sanksi finansial, larangan operasi, dan mekanisme pemulihan hukum untuk memastikan kepatuhan.[11]

Aksi Penegakan Privasi di Amerika Serikat: Penegakan privasi di Amerika Serikat lebih tersebar luas dan seringkali dicapai melalui penyelesaian kasus dengan Federal Trade Commission (FTC) atau tindakan hukum oleh jaksa agung negara bagian. Ini berbeda dengan metode terpusat di Uni Eropa. Penyelesaian FTC dengan Facebook pada tahun 2019 adalah salah satu kasus paling signifikan di mana organisasi dikenai denda sebesar $5 miliar karena melanggar perjanjian privasi sebelumnya setelah skandal Cambridge Analytica. Selain itu, perusahaan seperti Google dan YouTube juga telah dihukum oleh Federal Trade Commission karena melanggar Children's Online Privacy Protection Act (COPPA). Salah satu contohnya adalah denda sebesar $170 juta pada tahun 2019 karena mengumpulkan data anak-anak tanpa persetujuan orang tua.

California adalah salah satu dari banyak negara bagian yang melaksanakan California Consumer Privacy Act (CCPA) dan versi revisinya, CPRA. Ini termasuk sanksi yang dijatuhkan pada Sephora pada tahun 2022 karena tidak mengikuti sinyal pengendalian privasi internasional dan tidak menunjukkan transparansi dalam penjualan data pengguna. Pengaturan data broker dan upaya pemerintah untuk memperketat penjualan data sensitif juga menjadi subjek kontroversi publik di bidang pengawasan pemerintah. Kontroversi ini sebagian dihentikan oleh perubahan kebijakan administrasi tertentu.

Selain tindakan perdata dan administratif, litigasi kelas—juga dikenal sebagai litigasi tindakan kelas—menjadi bagian penting dari penegakan privasi di Amerika Serikat. Contohnya adalah gugatan terhadap Equifax setelah pelanggaran data besar tahun 2017 yang

[11] Ghazali Hasan Nasakti, *IUS CONSTITUENDUM PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH DALAM INDUSTRI DAN PENEGAKAN HUKUM DI INDONESIA*, t.t.

mengungkap informasi tentang lebih dari 140 juta warga AS, yang menghasilkan penyelesaian senilai lebih dari $575 juta. Tidak seperti UE, pola penegakan ini menggambarkan gaya Amerika yang sangat dipengaruhi oleh kekuatan pasar, litigasi perdata, dan perubahan politik.

| **Aspek** | **Uni Eropa (GDPR)** | **Amerika Serikat (Sektoral + FTC + Negara Bagian)** |
|---|---|---|
| **Sistem Hukum** | Regulasi terpadu berbasis hak (GDPR), penegakan terpusat dan nasional | Model sektoral, multi-regulator (FTC, regulator sektor, AG negara bagian), serta litigasi perdata |
| **Contoh Kasus Utama** | Amazon – €746 juta (Luksemburg) karena pelanggaran persetujuan iklan personalisasi | Facebook – $5 miliar (FTC) akibat pelanggaran privasi dan kasus Cambridge Analytica |
| **Contoh Kasus Lain** | Meta/Facebook – denda miliaran euro atas pelanggaran transfer data & persetujuan | Google/YouTube – $170 juta (FTC) karena pelanggaran COPPA terkait data anak |
| **Kasus Data Biomterik** | Clearview AI – denda & larangan operasi di beberapa negara Eropa karena scraping data wajah tanpa izin | Clearview AI – gugatan negara bagian & class actions, namun tetap beroperasi (tidak ada larangan nasional) |
| **Kasus Konsumen** | TikTok – investigasi dan denda di UE terkait transparansi dan data anak | Equifax – penyelesaian >$575 juta akibat pelanggaran data besar (class action & FTC) |
| **Penegakan Negara Bagian** | Otoritas perlindungan data nasional + EDPB koordinasi lintas UE | California v. Sephora – penegakan CCPA/CPRA karena kegagalan menghargai Global Privacy Control |
| **Mekanisme Penegakan** | Investigasi administratif, audit, larangan operasi, denda proporsional (maks 4% omzet global) | Penyelesaian FTC, litigasi class-action, denda sektoral, injunctive relief |
| **Filosofi Penegakan** | Perlindungan data adalah hak fundamental, penekanan pada pencegahan & akuntabilitas | Fokus konsumen & praktik bisnis adil (*unfair/deceptive practices*) lebih dari hak privasi individu |
| **Outcome** | Denda bernilai besar + pembatasan | Denda besar, settlement jangka |

| | | |
|---|---|---|
| **Umum** | operasional & compliance ketat | panjang, namun lebih fleksibel terhadap inovasi bisnis |

**7. Diskusi**

Konsep privasi sebagai hak asasi manusia (UE) dibandingkan dengan privasi sebagai perlindungan konsumen dan kebebasan pasar (AS) adalah dasar perselisihan antara sistem AS dan filosofi GDPR. Sementara model Uni Eropa memiliki keseimbangan yang kuat antara kepentingan individu dan kontrol negara atas perusahaan digital, model Amerika Serikat memungkinkan eksplorasi teknologi tetapi menimbulkan risiko penyalahgunaan data. Transfer data, standar keamanan, perlindungan data sensitif, dan transparansi algoritmik membutuhkan harmonisasi lintas yurisdiksi. Di era ekonomi data, interoperabilitas di seluruh dunia menjadi masalah.

Teknologi AI & Pemrosesan Profiling: AS belum memiliki kerangka nasional yang konsisten untuk pengawasan AI terkait privasi, meskipun GDPR menuntut DPIA untuk pemrosesan berisiko tinggi.

Data Broker & Ekonomi Periklanan: Model bisnis yang bergantung pada pengumpulan dan penjualan data menimbulkan ketidakpastian hukum, dan beberapa negara bagian berusaha untuk memperbaiki ketidakpastian ini.

Politik & Penegakan: Konsistensi penegakan di Amerika Serikat dipengaruhi oleh perubahan kebijakan lintas pemerintahan. Ini termasuk perubahan pada prioritas CFPB/FTC. Selain itu, di Uni Eropa, pendekatan koordinatif antara otoritas nasional dan EDPB menghadapi masalah sumber daya. Hinshaw and Culbertson LLP+1

Rekomendasi praktis untuk organisasi internasional yang bekerja di kedua wilayah adalah sebagai berikut:

- menggunakan dasar yang sesuai dengan GDPR. GDPR mengurangi risiko di seluruh dunia karena memiliki peraturan paling ketat di seluruh dunia. GDPR
- peta aliran data dan segmentasi data. Untuk memetakan kewajiban sektoral dan negara bagian, lakukan inventarisasi data, atau peta aliran data.

Mengikuti Klausul Kontrak Standar (SCC) dan mengurangi transfer. Setiap kali data dikirim dari Uni Eropa, pastikan mekanisme transfer dan evaluasi telah dilakukan untuk memastikan bahwa hukum negara tujuan dipatuhi.

Privacy oleh desain dan DPIA Implementasikan kontrol organisasi dan teknis serta DPIA untuk pemrosesan berisiko tinggi (seperti pengambilan keputusan otomatis dan profiling skala besar). GDPR.

fleksibel terhadap perubahan undang-undang AS. Monitor undang-undang dan inisiatif federal (mis. ADPPA atau proposal lainnya) karena situasi di Amerika Serikat berkembang dengan cepat; siapkan rencana tindakan yang cepat untuk menanggapi undang-undang baru.

## D. KESIMPULAN

Dalam hal perlindungan data, Uni Eropa dan Amerika Serikat memiliki dua paradigma yang berbeda. GDPR menerapkan standar ketat dan sanksi keras untuk melindungi hak asasi data. Amerika Serikat mengambil pendekatan adaptif sektoral dan negara bagian, yang mendorong inovasi tetapi juga menyebabkan fragmentasi. Metode untuk memastikan kepatuhan perusahaan di seluruh dunia dimulai dengan mengadopsi GDPR sebagai dasar dan kemudian disesuaikan dengan persyaratan negara bagian dan sektoral di Amerika Serikat. Untuk membangun arsitektur tata kelola data global yang melindungi hak individu tanpa menghambat kemajuan teknologi, diperlukan diskusi transatlantik dan persetujuan prinsip inti.

Kajian komparatif ini menunjukkan bahwa Uni Eropa dan Amerika Serikat memiliki dua paradigma konseptual, normatif, dan kelembagaan untuk peraturan perlindungan data pribadi. Peraturan Perlindungan Data Umum (GDPR) Uni Eropa membangun sistem hukum yang komprehensif, konsisten, dan berbasis hak asasi dengan menempatkan perlindungan data sebagai hak dasar warga negara, seperti yang dinyatakan dalam Charter of Fundamental Rights of the European Union. Mekanisme kelembagaan yang diawasi oleh European Data Protection Board (EDPB) memberikan dukungan untuk kerangka ini dan memiliki otoritas untuk melakukan tindakan tegas, seperti mengeluarkan sanksi administratif yang signifikan, memberikan instruksi untuk memperbaiki kesalahan, dan membatasi pemrosesan data terhadap individu yang melanggar peraturan.

Sebaliknya, Amerika Serikat menggunakan pendekatan yang fragmentatif dan sektoral berdasarkan undang-undang federal khusus sektor, wewenang Federal Trade Commission untuk mengawasi sektor, dan undang-undang privasi negara bagian, terutama California Consumer Privacy Act (CCPA) dan California Privacy Rights Act (CPRA). Model ini mendorong kemajuan teknologi dan memberikan pelaku usaha fleksibilitas. Namun, kurangnya undang-undang privasi federal yang komprehensif menyebabkan standar perlindungan yang berbeda,

ketidakpastian tentang kepatuhan lintas yurisdiksi, dan tingkat perlindungan hak individu yang tidak konsisten.

Ada kelebihan dan kekurangan dari masing-masing metode. GDPR melindungi hak subjek data dengan standar perlindungan yang tinggi dan keyakinan hukum. Namun, rezim kepatuhan yang ketat dapat menyebabkan beban administratif dan biaya yang besar bagi bisnis, terutama yang berukuran menengah ke bawah. Sebaliknya, undang-undang AS mendorong ekonomi digital dan praktik kreatif, tetapi berpotensi menimbulkan kesenjangan perlindungan hukum dan risiko privasi yang lebih besar bagi orang-orang.

Dalam konteks operasi internasional, pendekatan yang paling efisien bagi perusahaan lintas negara adalah menggunakan GDPR sebagai dasar operasional (framework kepatuhan dasar), sambil mempertahankan persyaratan sektoral dan negara bagian AS. Metode ini meminimalkan risiko hukum lintas yurisdiksi sekaligus memberikan fondasi kepatuhan yang kuat.

Untuk memperkuat tata kelola data global di masa depan, diperlukan kolaborasi kebijakan antara kedua yurisdiksi. Ini terutama berkaitan dengan masalah transfer data lintas negara, penerapan definisi data sensitif yang konsisten, sistem pengawasan pemrosesan berisiko tinggi, dan peningkatan hak subjek data. Tanpa harus menyatukan sistem secara keseluruhan, harmonisasi prinsip-prinsip dasar dapat menghasilkan ekosistem perlindungan data yang lebih baik, menjamin kepastian hukum bagi pelaku usaha, dan mendorong inovasi teknologi yang bijaksana di era ekonomi digital.

Oleh karena itu, pendekatan kebijakan yang ideal bukanlah memilih antara model Eropa dan Amerika Serikat; sebaliknya, mereka harus membangun pendekatan hibrida yang menggabungkan perlindungan hak individu yang kuat dengan fleksibilitas regulasi yang dapat disesuaikan untuk menjamin keseimbangan antara kepentingan perlindungan data pribadi, kemajuan teknologi, dan persaingan ekonomi global.

## E. DAFTAR PUSTAKA

Ardyan, Elia, Yoseb Boari, Akhmad Akhmad, dkk. METODE PENELITIAN KUALITATIF DAN KUANTITATIF : Pendekatan Metode Kualitatif dan Kuantitatif di Berbagai Bidang. PT. Sonpedia Publishing Indonesia, 2023.

Ayiliani, Fanisa Mayda, dan Elfia Farida. “Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara.” Jurnal Pembangunan Hukum Indonesia 6, no. 3 (2024): 431–55.

https://doi.org/10.14710/jphi.v6i3.%p.

Faizah, Azza Fitrahul, Sinta Dewi Rosadi, Garry Gumelar Pratama, dan Ananda Fersa Dharmawan. "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura." Hakim: Jurnal Ilmu Hukum Dan Sosial 1, no. 3 (2023): 01–27. https://doi.org/10.51903/hakim.v1i3.1222.

Hilma, Qurratul. "INTEGRASI GENERAL DATA PROTECTION REGULATION DALAM REGULASI PRIVASI DATA: SOLUSI TANTANGAN TEKNOLOGI KECERDASAN BUATAN." Jurnal Legislatif, 9 Oktober 2025, 95–112. https://doi.org/10.20956/jl.v8i2.44141.

Idat, Dhani Gunawan. "Memanfaatkan Era Ekonomi Digital Untuk Memperkuat Ketahanan Nasional." Jurnal Lemhannas RI 7, no. 2 (2019): 5–11. https://doi.org/10.55960/jlri.v7i2.67.

Kusumadewi, Dzikrina Laili, dan Akhmad Cahyono. "Urgensi Perlindungan Data Pribadi Pada Sistem Elektronik Untuk Anak Di Bawah Umur Di Indonesia Serta Perbandingan Regulasi Dengan Uni Eropa (General Data Protection Regulation)." Lex Patrimonium 2, no. 2 (2023). https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/12.

Leonora, Gracella, dan Roy Vincentius Pratikno. "REGULASI PERDAGANGAN TERKAIT PERLINDUNGAN PRIVASI KONSUMEN DALAM EKSPANSI BISNIS DI UNI EROPA: STUDI KASUS ALIBABA." Verity: Jurnal Ilmiah Hubungan Internasional (International Relations Journal) 16, no. 32 (2024): 25–43. europe. https://doi.org/10.19166/verity.v16i32.9101.

Mubarikah, Nurul. "KEWAJIBAN ENDORSER ATAS PENGANJURAN SUATU PRODUK PADA MEDIA SOSIAL MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA DALAM PERBANDINGAN DENGAN AMERIKA SERIKAT, INGGRIS DAN INDIA." "Dharmasisya" Jurnal Program Magister Hukum FHUI 1, no. 1 (2021). https://scholarhub.ui.ac.id/dharmasisya/vol1/iss1/13.

Nasakti, Ghazali Hasan. IUS CONSTITUENDUM PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH DALAM INDUSTRI DAN PENEGAKAN HUKUM DI INDONESIA. t.t.

Pradana, Muhammad Akbar Eka, dan Horadin Saragih. "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya." Innovative: Journal Of Social Science Research 4, no. 4 (2024): 3412–25. https://doi.org/10.31004/innovative.v4i4.13476.

Varany, Yacinta Tira, dan Listyowati Sumanto. "Dinamika Sistem Hukum Pelindungan Data

Pribadi: Analisis Interaksi Struktur, Substansi, Dan Kultur Hukum Di Era Big Data." Jurnal Impresi Indonesia 4, no. 11 (2025): 5172–85. https://doi.org/10.58344/jii.v4i11.7182.