JAKSA
Jurnal Kajian Ilmu Hukum dan Politik

LPPM Universitas Sains dan Teknologi Komputer
Vol. 2 No. 4 Oktober 2024, Hal. 45-56
e-ISSN: 2988-5140 ; p-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/Jaksa

Tanggung Jawab Hukum Perusahaan Teknologi Atas Penyalahgunaan Data Pengguna : Studi Kasus Di ASEAN

Maulana Fahmi Idris*[1], Joni Laksito[2], Widya Ariyani[3]
[1]*Universitas Sains dan Teknologi Komputer Semarang, maulanafahmi@stekom.ac.id*
[2]*Universitas Sains dan Teknologi Komputer Semarang, jonilaksito@gmail.com*
[3]*Universitas Sains dan Teknologi Komputer Semarang, widya.ariyani@stekom.ac.id*

Abstract
This study examines the legal responsibility of technology companies in protecting user data in the ASEAN region amidst the increasing risks of data misuse in the digital era. The research adopts a qualitative approach, analyzing existing data protection regulations in Indonesia, Malaysia, and Hong Kong, and compares these to the General Data Protection Regulation (GDPR) in the European Union. The findings reveal significant regulatory disparities within ASEAN, with countries facing challenges in enforcement and public awareness regarding data privacy. Case studies of data breaches highlight the need for stronger security measures and transparency from technology companies to protect user data. Additionally, this study underscores the importance of regional collaboration among ASEAN countries to establish harmonized and effective data protection standards that align with global best practices. Strengthening data protection regulations and enforcement mechanisms can foster a safer digital environment, promoting user trust and supporting sustainable digital economic growth in the region.

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

I. INTRODUCTION

Di era digital saat ini, penggunaan data pribadi telah menjadi bagian integral dari operasi bisnis perusahaan teknologi, terutama yang bergerak di bidang internet dan layanan berbasis data (Paramesha et al., 2024). Data pribadi pengguna, yang meliputi informasi identitas, lokasi, preferensi, dan perilaku, memiliki nilai ekonomi yang tinggi bagi perusahaan teknologi yang memanfaatkan data tersebut untuk berbagai tujuan, mulai dari peningkatan layanan hingga pemasaran yang ditargetkan (Okorie et al., 2024). Namun, perkembangan ini juga menimbulkan kekhawatiran terhadap privasi dan keamanan data, terutama ketika data tersebut disalahgunakan atau tidak dikelola dengan bijaksana oleh perusahaan teknologi (Zhu & Song, 2022).

Isu terkait tanggung jawab hukum perusahaan teknologi dalam pengelolaan data pengguna semakin penting karena banyaknya kasus kebocoran dan penyalahgunaan data yang merugikan individu maupun masyarakat luas (Andrew et al., 2023). Dalam beberapa tahun terakhir, kasus-kasus ini menarik perhatian global, khususnya di negara-negara ASEAN, di mana peraturan perlindungan data masih beragam dan sebagian besar masih dalam tahap perkembangan (Calzada, 2022). Di Indonesia misalnya, regulasi baru mengenai perlindungan data pribadi mulai diimplementasikan, tetapi masih menghadapi berbagai tantangan dalam pelaksanaannya (Sudarwanto & Kharisma, 2022).

Submitted: September 29, 2024 , Reviewed: Oktober 20, 2024, Accepted: Oktober 29, 2024

Regulasi terkait perlindungan data pribadi di ASEAN sangat bervariasi dalam pendekatan dan penerapannya (Morgan, 2022). Di Indonesia, perlindungan data diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) yang menekankan hak individu atas data pribadi serta kewajiban perusahaan dalam menjaga kerahasiaannya (Alibeigi et al., 2022). Di Malaysia, peraturan yang berlaku adalah Personal Data Protection Act yang menitikberatkan pada perlindungan dalam sektor komersial (Cheryl & Ng, 2022). Sebaliknya, Hong Kong menggunakan Personal Data (Privacy) Ordinance yang lebih berfokus pada transparansi proses pengumpulan dan penyimpanan data, serta mekanisme pengawasan yang lebih ketat dalam mengelola informasi pribadi (Chen & Yang, 2022). Perbedaan ini menunjukkan bahwa negara-negara ASEAN memiliki kerangka hukum yang berbeda dalam melindungi data pengguna, dan masih berjuang untuk mencapai standar perlindungan yang memadai.

Penyalahgunaan data pengguna sering kali terjadi akibat lemahnya sistem keamanan serta kebijakan yang kurang memadai dalam perusahaan teknologi. Data pribadi pengguna kerap dimanfaatkan secara tidak sah oleh pihak yang tidak bertanggung jawab, baik untuk kepentingan komersial maupun tindakan kriminal siber. Kondisi ini diperparah dengan rendahnya kesadaran perusahaan dalam memperhatikan privasi dan keamanan data pengguna, serta adanya celah dalam regulasi yang dimanfaatkan untuk mengakses data secara ilegal (Ismagilova et al., 2022). Misalnya, menurut Sheng et al. (2023), banyak individu yang mengalami kehilangan privasi, risiko keuangan, hingga tekanan emosional akibat penyalahgunaan data pribadi mereka. Risiko ini semakin meningkat ketika data yang dikumpulkan dan disimpan tidak terlindungi dengan baik, sehingga mengundang berbagai ancaman siber yang dapat merugikan pengguna (Santoso et al., 2024).

Di sisi lain, dampak penyalahgunaan data pengguna tidak hanya dirasakan oleh individu yang kehilangan privasinya, tetapi juga memengaruhi perusahaan teknologi itu sendiri serta masyarakat luas (Pyrrho et al., 2022). Bagi perusahaan, kebocoran data dapat mengakibatkan hilangnya kepercayaan publik dan penurunan reputasi. Pengguna yang merasa datanya tidak aman akan cenderung enggan menggunakan layanan perusahaan tersebut, yang pada akhirnya berdampak pada keuntungan bisnis (Wylde et al., 2022). Selain itu, ketidakpercayaan masyarakat terhadap perusahaan teknologi akibat penyalahgunaan data dapat memperlambat adopsi teknologi baru dan menghambat pertumbuhan ekonomi digital, yang sangat bergantung pada kepercayaan pengguna dalam berbagi data. Bagi masyarakat, penyalahgunaan data tidak hanya menyebabkan kerugian finansial dan privasi, tetapi juga menurunkan tingkat kepercayaan terhadap teknologi yang seharusnya meningkatkan kualitas hidup mereka (Nampewo et al., 2022).

Secara global, General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa menjadi contoh regulasi ketat yang melindungi data pengguna dengan standar keamanan tinggi dan sanksi signifikan bagi perusahaan yang melanggar (Fiero & Beier, 2022). GDPR menetapkan ketentuan bahwa perusahaan harus mendapatkan persetujuan eksplisit dari pengguna sebelum mengumpulkan

dan menggunakan data pribadi mereka (Seun Solomon Bakare et al., 2024). Banyak negara di Asia Tenggara yang mulai menjadikan GDPR sebagai acuan dalam memperkuat regulasi perlindungan data mereka, meskipun penerapannya belum seketat di Eropa (Bentotahewa et al., 2022). Dengan demikian, perusahaan teknologi di ASEAN perlu untuk tidak hanya mematuhi regulasi lokal tetapi juga mengadopsi praktik terbaik internasional guna melindungi data pengguna dan memperkuat kepercayaan publik (Curtis et al., 2022).

Tanggung jawab hukum perusahaan teknologi dalam melindungi data pengguna menjadi semakin penting untuk memastikan bahwa data pribadi dikelola dengan aman dan transparan (Asgarinia et al., 2023). Menurut Beccia et al. (2022), tanggung jawab hukum mencakup kewajiban perusahaan untuk memastikan bahwa sistem keamanan mereka cukup kuat untuk mencegah akses yang tidak sah dan bahwa pengumpulan serta pemrosesan data dilakukan dengan persetujuan yang jelas dari pengguna. Di banyak negara, tanggung jawab hukum ini diatur melalui undang-undang yang bertujuan untuk melindungi privasi dan keamanan data pengguna, seperti GDPR di Eropa dan UU PDP di Indonesia (Dehbi & Martin-Ortega, 2023). Selain mematuhi regulasi yang ada, perusahaan teknologi juga harus menerapkan teknologi enkripsi, autentikasi ganda, dan pemantauan aktivitas jaringan sebagai langkah preventif terhadap akses ilegal. Di samping itu, transparansi dalam kebijakan privasi dan pemberian kontrol yang lebih besar kepada pengguna atas data mereka adalah langkah penting dalam menunjukkan tanggung jawab perusahaan terhadap hak-hak pengguna (Omotunde & Ahmed, 2023).

Dalam konteks ASEAN, pendekatan untuk melindungi data pengguna cenderung lebih adaptif dan berorientasi pada kolaborasi antar negara, berbeda dengan pendekatan terstruktur GDPR di Uni Eropa (Metcalf & Papageorgiou, 2022). Menurut Chen & Yang (2022), ASEAN lebih mengedepankan kolaborasi antar negara anggota dan penguatan kapasitas dalam menghadapi isu keamanan siber, sementara Uni Eropa menerapkan regulasi yang ketat melalui GDPR yang berlaku bagi seluruh negara anggota (A Bimantara, 2022). Pendekatan ASEAN yang lebih desentralisasi ini menekankan pada sinergi antar negara untuk mengatasi isu-isu keamanan siber, tetapi kurang dalam hal penegakan regulasi yang seragam, yang memungkinkan adanya perbedaan dalam perlindungan data di setiap negara (Radanliev, 2024). Sebagai contoh, meskipun Malaysia telah mengimplementasikan Undang-Undang Perlindungan Data Pribadi sejak 2010, penerapannya masih terkendala kurangnya penegakan yang efektif dan rendahnya kesadaran masyarakat mengenai pentingnya perlindungan data. Sebaliknya, Indonesia baru-baru ini mengesahkan UU PDP yang diharapkan dapat memperbaiki sistem perlindungan data di negara tersebut, meskipun pelaksanaannya masih menghadapi banyak tantangan (Widiatedja & Mishra, 2023).

Penelitian ini bertujuan untuk mengkaji tanggung jawab hukum perusahaan teknologi dalam melindungi data pengguna dengan fokus pada negara-negara ASEAN. Dengan mengidentifikasi peran perusahaan dalam pencegahan penyalahgunaan data serta bagaimana regulasi dapat diperkuat untuk melindungi hak-hak pengguna, penelitian ini diharapkan dapat memberikan kontribusi pada literatur

mengenai hukum perlindungan data di kawasan ASEAN. Selain itu, penelitian ini diharapkan dapat memberikan rekomendasi bagi perusahaan teknologi untuk menerapkan standar keamanan yang sesuai dengan praktik terbaik internasional. Dalam lingkungan digital yang semakin kompleks, perlindungan data pengguna tidak hanya menjadi tanggung jawab individu atau pemerintah, tetapi juga perusahaan teknologi yang harus bertindak proaktif dalam melindungi data yang mereka kelola (Nguyen & Tran, 2019).

Kesadaran mengenai pentingnya perlindungan data diharapkan semakin meningkat di kalangan pemerintah, perusahaan, dan pengguna itu sendiri. Pengguna diharapkan lebih berhati-hati dalam memberikan informasi pribadi serta lebih cermat memahami syarat dan ketentuan penggunaan data yang ditetapkan oleh perusahaan teknologi (Shahid et al., 2022). Dengan adanya kesadaran yang lebih besar, regulasi yang ketat, dan sistem keamanan yang kuat, potensi penyalahgunaan data pengguna dapat diminimalisir, dan peningkatan kepercayaan publik terhadap teknologi digital akan mendorong pertumbuhan ekonomi digital yang lebih sehat dan berkelanjutan (Justine Chilenovu Ogborigbo et al., 2024).

II. METHODOLOGY

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk mengkaji tanggung jawab hukum perusahaan teknologi dalam perlindungan data pengguna di kawasan ASEAN.

A. Desain Penelitian

Metode kualitatif dipilih karena memungkinkan analisis mendalam terhadap isu hukum, kebijakan privasi, serta regulasi perlindungan data di berbagai negara ASEAN.

B. Prosedur Pengumpulan Data

Dalam konteks ini, penelitian mengandalkan data sekunder berupa dokumentasi regulasi, literatur akademis, laporan dari lembaga pemerintahan, dan studi kasus dari beberapa negara anggota ASEAN.

C. Instrumen Penelitian

Data yang digunakan dalam penelitian ini dikumpulkan melalui kajian pustaka dan analisis dokumen. Sumber-sumber utama termasuk regulasi perlindungan data, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, Personal Data Protection Act (PDPA) di Malaysia, serta Personal Data (Privacy) Ordinance di Hong Kong (Sudarwanto & Kharisma, 2022). Selain itu, penelitian juga mengacu pada literatur akademis dan artikel jurnal yang relevan, yang membahas isu privasi, keamanan data, dan tanggung jawab perusahaan teknologi dalam pengelolaan data pengguna. Data dari sumber-sumber ini dianalisis untuk memahami variasi dalam pendekatan regulasi, implementasi, dan tantangan yang dihadapi oleh masing-masing negara dalam melindungi data pengguna (Chen & Yang, 2022).

D. Prosedur Analisis Data

Untuk memperkaya analisis, penelitian ini juga menggunakan studi kasus sebagai teknik analisis data. Studi kasus yang dipilih adalah kasus-kasus pelanggaran data yang melibatkan perusahaan teknologi besar di kawasan ASEAN. Pendekatan ini memberikan konteks praktis terhadap penerapan dan efektivitas regulasi perlindungan data di masing-masing negara. Studi kasus diidentifikasi berdasarkan laporan pelanggaran yang tersedia dalam publikasi pemerintah dan media yang kredibel, dan dianalisis untuk mengevaluasi sejauh mana perusahaan bertanggung jawab dalam melindungi data pengguna serta dampaknya terhadap konsumen dan reputasi perusahaan.

E. Langkah-Langkah Pelaksanaan (Opsional)

Analisis data dilakukan secara tematik untuk mengidentifikasi pola dan tren dalam regulasi perlindungan data di negara-negara ASEAN. Pendekatan tematik ini memungkinkan identifikasi tema utama seperti kebijakan transparansi, hak pengguna, dan tingkat penegakan hukum dalam perlindungan data. Setiap tema dianalisis berdasarkan perbandingan antara regulasi di masing-masing negara ASEAN dan standar internasional, khususnya General Data Protection Regulation (GDPR) di Uni Eropa. Analisis perbandingan ini bertujuan untuk mengidentifikasi kesenjangan dan peluang untuk memperkuat regulasi di ASEAN dengan mencontoh praktik terbaik internasional (Bentotahewa et al., 2022).

F. Pertimbangan Etis

Dalam menginterpretasi data, penelitian ini mengacu pada pendekatan analisis deskriptif yang fokus pada penyajian informasi yang akurat mengenai tanggung jawab hukum perusahaan teknologi di ASEAN. Melalui analisis ini, peneliti berusaha menggambarkan kondisi regulasi, praktik perusahaan, serta dampak sosial dari penyalahgunaan data pengguna. Setiap interpretasi didasarkan pada data empiris dari dokumen regulasi, literatur akademis, dan studi kasus, yang diharapkan mampu memberikan pandangan komprehensif tentang tantangan dan peluang dalam perlindungan data di ASEAN.

III. RESULT AND DUSCUSSION

Result

Bagian Result and Discussion sebaiknya disusun secara berurutan dan logis, sehingga pembaca dapat memahami hasil penelitian dan interpretasinya.

a. Regulasi Perlindungan Data di ASEAN

Pada tabel 1 berikut ditampilkan perbandingan regulasi perlindungan data pribadi di tiga negara ASEAN, yaitu Indonesia, Malaysia, dan Hong Kong. Setiap negara memiliki pendekatan berbeda dalam melindungi data pribadi pengguna, yang dipengaruhi oleh kerangka hukum masing-masing.

Tabel 1. Perbandingan regulasi perlindungan data pribadi di tiga negara ASEAN, yaitu Indonesia

Negara	Regulasi	Poin Kunci	Tingkat Penegakan
Indonesia	Undang-Undang Perlindungan Data Pribadi (UU PDP)	Fokus pada hak pengguna atas data pribadi dan kewajiban perusahaan untuk menjaga kerahasiaan.	Sedang
Malaysia	Personal Data Protection Act (PDPA)	Menekankan perlindungan data di sektor komersial, memerlukan persetujuan pengguna untuk pemrosesan data.	Sedang
Hongkong	Personal Data (Privacy) Ordinance	Mengutamakan transparansi dan pengawasan dalam pengumpulan serta penyimpanan data pribadi.	Tinggi

Berdasarkan tabel di atas, terlihat bahwa ketiga negara memiliki fokus yang berbeda dalam perlindungan data. Hong Kong memiliki tingkat penegakan yang tinggi, dengan pengawasan ketat melalui Personal Data (Privacy) Ordinance, sedangkan Indonesia dan Malaysia masih berada pada tingkat sedang, dengan beberapa tantangan dalam penegakan hukum (Sudarwanto & Kharisma, 2022).

b. Studi Kasus Pelanggaran Data di Perusahaan Teknologi

Beberapa kasus kebocoran data pengguna di perusahaan teknologi besar menunjukkan tantangan yang dihadapi negara-negara ASEAN dalam menegakkan regulasi perlindungan data. Berikut adalah contoh kasus pelanggaran data pengguna di Indonesia dan Malaysia.

Indonesia

Pada tahun 2023, sebuah perusahaan e-commerce mengalami kebocoran data yang berdampak pada jutaan pengguna. Data yang bocor termasuk nama, alamat, dan nomor kontak pengguna. Kebocoran ini mengindikasikan kurangnya sistem keamanan dan kepatuhan terhadap UU PDP, yang baru saja diimplementasikan. Kasus ini meningkatkan urgensi pengawasan regulasi lebih ketat di Indonesia (Sudarwanto & Kharisma, 2022).

Malaysia

Pada tahun 2022, terjadi pelanggaran data yang melibatkan perusahaan penyedia layanan komunikasi, di mana data pribadi pengguna diekspos tanpa persetujuan. Hal ini melanggar PDPA Malaysia, tetapi

penegakan hukum yang lemah mengakibatkan sanksi yang minimal. Kasus ini menunjukkan bahwa meskipun regulasi sudah ada, penegakannya masih menjadi tantangan besar (Cheryl & Ng, 2022).

c. Perbandingan Regulasi ASEAN dengan GDPR

Untuk memahami posisi ASEAN dalam konteks global, tabel 2 berikut ini menampilkan perbandingan aspek kunci dari regulasi di ASEAN dengan GDPR yang diterapkan di Uni Eropa.

Tabel 2. Perbandingan aspek kunci dari regulasi di asean dengan gdpr yang diterapkan di uni eropa.

Aspek Regulasi	ASEAN	GDPR (Uni Eropa)
Persetujuan Pengguna	Diperlukan Di Beberapa Negara	Persetujuan Eksplisit Wajib
Hak untuk Dilupakan	Belum diimplementasikan di sebagian besar negara	Diwajibkan dan Dilindungi Penuh
Transparansi dan Akses Data	Variatif, tergantung pada regulasi masing-masing negara	Standar transparansi tinggi dan akses penuh
Penegakan dan Sanksi	Terbatas pada denda rendah di beberapa negara	Denda Tinggi dan Sanksi Berat

Dari tabel tersebut di atas, menunjukkan bahwa Perbedaan signifikan antara GDPR dan regulasi di ASEAN terlihat dari tingkat transparansi, hak pengguna, serta penegakan hukum. GDPR menetapkan standar yang lebih tinggi dibandingkan dengan regulasi ASEAN, yang sering kali masih dalam tahap perkembangan dan belum memiliki penegakan yang kuat (Bentotahewa et al., 2022).

Discussion

Berdasarkan hasil analisis regulasi dan studi kasus, terdapat beberapa poin penting yang perlu diperhatikan terkait tanggung jawab hukum perusahaan teknologi dalam melindungi data pengguna di ASEAN. Perusahaan teknologi memiliki peran penting dalam menjaga data pribadi pengguna, namun regulasi yang ada di ASEAN masih memiliki beberapa kelemahan. Dibandingkan dengan GDPR, regulasi ASEAN kurang memberikan hak yang kuat kepada pengguna, seperti hak untuk dilupakan dan hak akses penuh terhadap data pribadi.

Tantangan utama dalam penerapan perlindungan data di ASEAN adalah kurangnya standar yang seragam dan tingkat penegakan yang bervariasi. Hal ini terlihat pada kasus di Indonesia dan Malaysia, di mana kebocoran data sering kali terjadi akibat lemahnya sistem keamanan internal perusahaan dan penegakan regulasi yang kurang efektif. Meskipun UU PDP di Indonesia dan PDPA di Malaysia sudah mengatur perlindungan data, penerapan di lapangan menunjukkan masih adanya celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab (Sudarwanto & Kharisma, 2022).

Di sisi lain, Uni Eropa melalui GDPR berhasil menetapkan standar yang tinggi dalam perlindungan data, terutama dalam penegakan sanksi yang ketat terhadap pelanggaran data pribadi. Perbandingan ini menunjukkan adanya peluang bagi negara-negara ASEAN untuk memperkuat regulasi mereka dengan mengadopsi elemen-elemen penting dari GDPR, seperti persyaratan persetujuan eksplisit, hak untuk dilupakan, dan penegakan yang lebih tegas (Chen & Yang, 2022). Dengan meniru praktik terbaik internasional, ASEAN dapat menciptakan lingkungan digital yang lebih aman bagi pengguna (Bentotahewa et al., 2022).

Hasil penelitian ini menunjukkan bahwa tanggung jawab hukum perusahaan teknologi dalam melindungi data pengguna sangat bergantung pada regulasi dan penegakan hukum yang kuat. Perusahaan teknologi perlu mengadopsi standar keamanan yang lebih tinggi dan berupaya meningkatkan transparansi serta kontrol pengguna atas data mereka. Selain itu, pemerintah ASEAN harus berperan lebih aktif dalam meningkatkan kesadaran masyarakat tentang pentingnya privasi data dan mendorong perusahaan untuk menerapkan sistem keamanan yang memadai.

Penelitian ini juga menyoroti pentingnya kolaborasi antarnegara ASEAN dalam menciptakan regulasi yang lebih harmonis dan efektif. Dengan adanya kerja sama regional, diharapkan regulasi perlindungan data di ASEAN dapat lebih seragam dan mampu bersaing dengan standar global seperti GDPR. Kolaborasi ini juga berpotensi meningkatkan kepercayaan pengguna terhadap teknologi digital dan mendorong pertumbuhan ekonomi digital yang berkelanjutan di kawasan ASEAN.

IV. CONCLUSION

Penelitian ini menyoroti pentingnya tanggung jawab hukum perusahaan teknologi dalam melindungi data pribadi pengguna di tengah meningkatnya risiko penyalahgunaan data di era digital. Berdasarkan analisis terhadap regulasi perlindungan data di beberapa negara ASEAN, terlihat bahwa kerangka hukum di kawasan ini masih beragam dan belum memiliki standar penegakan yang seketat GDPR di Uni Eropa. Meskipun negara-negara seperti Indonesia dan Malaysia telah mengimplementasikan regulasi perlindungan data, efektivitasnya masih terbatas akibat lemahnya sistem penegakan dan rendahnya kesadaran masyarakat akan pentingnya privasi data.

Temuan penelitian ini juga menunjukkan bahwa perusahaan teknologi memiliki kewajiban besar untuk memastikan keamanan data pengguna melalui sistem yang kuat dan transparan. Kebocoran data yang terjadi di beberapa perusahaan besar di ASEAN mengindikasikan adanya kebutuhan mendesak bagi perusahaan untuk tidak hanya mematuhi regulasi yang ada tetapi juga menerapkan praktik terbaik dalam keamanan siber, seperti enkripsi dan autentikasi ganda. Selain itu, transparansi dalam kebijakan privasi serta pemberian kontrol lebih besar kepada pengguna atas data mereka adalah langkah penting dalam memperkuat kepercayaan publik.

Dalam konteks ASEAN, masih terdapat kesenjangan antara regulasi perlindungan data dan standar internasional seperti GDPR. Oleh karena itu, kolaborasi antarnegara ASEAN sangat penting untuk

menciptakan regulasi yang lebih harmonis dan efektif, yang mampu melindungi hak-hak pengguna serta mendorong pertumbuhan ekonomi digital yang berkelanjutan. Dengan mengadopsi elemen-elemen kunci dari GDPR, negara-negara ASEAN dapat memperkuat sistem perlindungan data mereka dan mendorong perusahaan untuk lebih bertanggung jawab dalam pengelolaan data pengguna.

Peningkatan kualitas regulasi dan penegakan hukum, serta komitmen perusahaan teknologi dalam melindungi data pengguna, adalah langkah penting untuk menciptakan lingkungan digital yang aman dan dapat dipercaya di ASEAN. Penelitian ini diharapkan dapat berkontribusi dalam mendorong perbaikan regulasi perlindungan data di ASEAN dan meningkatkan kesadaran perusahaan teknologi mengenai tanggung jawab hukum mereka dalam menjaga privasi pengguna.

REFERENCES

A Bimantara. (2022). The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices. *Global: Jurnal Politik Internasional*, *24*(1). https://doi.org/10.7454/global.v24i1.684

Alibeigi, A., Munir, A. B., & Asemi, A. (2022). A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle. *Journal of Data Protection and Privacy*, *5*(2), 119–137. https://doi.org/10.69554/yqug8122

Andrew, J., Baker, M., & Huang, C. (2023). Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play? *Critical Perspectives on Accounting*, *90*. https://doi.org/10.1016/j.cpa.2021.102396

Asgarinia, H., Chomczyk Penedo, A., Esteves, B., & Lewis, D. (2023). "Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information (Switzerland)*, *14*(7). https://doi.org/10.3390/info14070351

Beccia, F., Rossi, M. F., Amantea, C., Villani, L., Daniele, A., Tumminello, A., Aristei, L., Santoro, P. E., Borrelli, I., Ricciardi, W., Gualano, M. R., & Moscato, U. (2022). COVID-19 Vaccination and Medical Liability: An International Perspective in 18 Countries. *Vaccines*, *10*(8). https://doi.org/10.3390/vaccines10081275

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science*, *3*(3). https://doi.org/10.1007/s42979-022-01079-z

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150. https://doi.org/10.3390/smartcities5030057

Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *International Spectator*, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Cheryl, B. K., & Ng, B. K. (2022). Protecting the Unprotected Consumer Data in Internet of Things: Current Scenario of Data Governance in Malaysia. *Sustainability (Switzerland)*, *14*(16). https://doi.org/10.3390/su14169893

Curtis, H., Hogeveen, B., Kang, J., Le Thu, H., Rajagopalan, R. P., & Ray, T. (2022). Digital Southeast Asia. In *Australian Strategic …* (Issue 57). www.aspi.org.au

Dehbi, F., & Martin-Ortega, O. (2023). An integrated approach to corporate due diligence from a human rights, environmental, and TWAIL perspective. *Regulation and Governance*, *17*(4), 927–943. https://doi.org/10.1111/rego.12538

Fiero, A. W., & Beier, E. (2022). New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation. *Stanford Journal of International Law. Summer2022*, *58*(2), 151–192. https://web.s.ebscohost.com/ehost/detail/detail?vid=43&sid=84cbea20-4a76-4b13-8276-f7e1c6d77d8c%40redis&bdata=JkF1dGhUeXBlPXNzbyZzY29wZT1zaXRl#AN=158842953&db=a9h

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*, *24*(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Justine Chilenovu Ogborigbo, Odunayo Sekinat Sobowale, Emmanuel Iyere Amienwalen, Yemisi Owoade, Adeyemo Taiwo Samson, & Joshua Egerson. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. *World Journal of Advanced Research and Reviews*, *23*(1), 081–096. https://doi.org/10.30574/wjarr.2024.23.1.1900

Metcalf, K. N., & Papageorgiou, I. F. (2022). Increasing Trust in the Digital Market Through Regional Rules: the Case of Asia. *Asia Pacific Journal on Human Rights and the Law*, *23*(2), 245–279. https://doi.org/10.1163/15718158-23020004

Morgan, P. J. (2022). Fintech and Financial Inclusion in Southeast Asia and India. *Asian Economic Policy Review*, *17*(2), 183–208. https://doi.org/10.1111/aepr.12379

Nampewo, Z., Mike, J. H., & Wolff, J. (2022). Respecting, protecting and fulfilling the human right to health. *International Journal for Equity in Health*, *21*(1). https://doi.org/10.1186/s12939-022-

01634-3

Nguyen, M. T., & Tran, M. Q. (2019). Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices. *International Journal of Intelligent Automation and Computing*.

Okorie, G. N., Egieya, Z. E., Ikwue, U., Udeh, C. A., Adaga, E. M., DaraOjimba, O. D., & Oriekhoe, O. I. (2024). Leveraging big data for personalized marketing campaigns: a review. *International Journal of Management & Entrepreneurship Research*, *6*(1), 216–242.

Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115–133. https://doi.org/10.58496/MJCS/2023/016

Paramesha, M., Rane, N., & Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4855856

Pyrrho, M., Cambraia, L., & de Vasconcelos, V. F. (2022). Privacy and Health Practices in the Digital Age. *American Journal of Bioethics*, *22*(7), 50–59. https://doi.org/10.1080/15265161.2022.2040648

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. https://doi.org/10.1080/23742917.2024.2312671

Santoso, J. T., Raharjo, B., & Wibowo, A. (2024). Combination of Alphanumeric Password and Graphic Authentication for Cyber Security. *Journal of Internet Services and Information Security*, *14*(1), 16–36. https://doi.org/10.58346/JISIS.2024.I1.002

Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). Data Privacy Laws and Compliance: a Comparative Review of the Eu Gdpr and Usa Regulations. *Computer Science & IT Research Journal*, *5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

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

Sheng, N., Yang, C., Han, L., & Jou, M. (2023). Too much overload and concerns: Antecedents of social media fatigue and the mediating role of emotional exhaustion. *Computers in Human Behavior*, *139*. https://doi.org/10.1016/j.chb.2022.107500

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: a future–forward perspective. *International Review of Law, Computers and Technology*, *37*(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2). https://doi.org/10.1007/s42979-022-01020-4

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