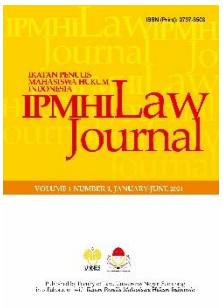
IKATAN PENULIS MAHASISWA HUKUM INDONESIA LAW JOURNAL



ISSN 2797-8508 (Print)
ISSN 2807-8330 (Online)
VOL. 4 NO. 1, JANUARY (2024)

Riwayat Artikel
History of Article
Diajukan: 29 Desember 2023
Submitted
Direvisi: 7 Januari 2023
Revised
Diterima: 12 Januari 2024
Accepted

Saran Perujukan
How to cite:
Marischa, D., & Setianingrum, R. B. (2024). Transfer of Personal Data by E-Commerce Companies: A Study From The Perspective of Indonesian Personal Data Protection Laws. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *4*(1), 48-64. https://doi.org/10.15294/ipmhi.v4i1.78267

© 2024 Authors. This work is licensed under a Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0). All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions. This title has been indexed by Google Scholar

Transfer of Personal Data by E-Commerce Companies: A Study From The Perspective of Indonesian Personal Data Protection Laws

Transfer Data Pribadi oleh Perusahaan E-Commerce: Kajian Dari Perspektif Undang-undang Perlindungan Data Pribadi Indonesia

Diva Marischa[1], Reni Budi Setianingrum[2]
[1] Universitas Muhammadiyah Yogyakarta
[2] Universitas Muhammadiyah Yogyakarta

Email Korespondensi: divamarischa55@gmail.com

Abstract In the era of globalization, the protection of personal data has become a critical issue in Indonesia, especially within the e-commerce sector. Cases of this

nature underscore the significance of safeguarding personal data and enforcing stringent legal measures. This research employs a normative juridical legal study that integrates two primary approaches: the legislative approach and the comparative approach. The research data sources comprise primary, secondary, and tertiary legal materials obtained through a comprehensive literature review. The data analysis process is conducted using a descriptive method and applying deductive logic. The growth of e-commerce users in Indonesia has witnessed a significant increase. Law Number 27 of 2022 regulates the principles of personal data protection, encompassing the rights of data owners, transparency, and meticulous data management. While considered positive, a comparison with Malaysian regulations, such as the Personal Data Protection Act 2010, reveals fundamental differences that warrant attention. The implications of the regulation on the transfer of personal data in Law Number 27 of 2022 play a crucial role for e-commerce companies. They must ensure the security of consumers' personal data and adhere to legal principles to maintain consumer trust in an increasingly competitive market.

Keywords *E-Commerce; Protection of Personal Data; Data Transfer*

Abstrak Dalam era globalisasi, perlindungan data pribadi menjadi isu penting di Negara Indonesia, terutama dalam sektor *e-commerce*. Kasus semacam ini menekankan pentingnya perlindungan data pribadi dan penegakan hukum yang ketat. Penelitian ini menggunakan studi hukum yuridis normatif yang menggabungkan dua pendekatan utama, yakni pendekatan perundang-undangan dan komparatif. Sumber data penelitian terdiri dari bahan hukum primer, sekunder, dan tersier, yang diperoleh melalui studi kepustakaan. Proses analisis data dilakukan dengan menggunakan metode deskriptif dan menerapkan logika deduktif. Pertumbuhan pengguna *e-commerce* di Indonesia telah meningkat signifikan. Undang-Undang Nomor 27 Tahun 2022 mengatur prinsip-prinsip perlindungan data pribadi, seperti hak pemilik data, transparansi, dan manajemen data yang cermat. Meski dianggap positif, perbandingan dengan regulasi Malaysia, seperti *Personal Data Protection Act* 2010, menunjukkan perbedaan mendasar yang perlu diperhatikan. Implikasi regulasi transfer data pribadi dalam Undang-Undang No. 27 Tahun 2022 memainkan peran krusial bagi perusahaan *e-commerce*. Mereka harus menjaga keamanan data pribadi konsumen dan mematuhi prinsip-prinsip undang-undang untuk mempertahankan kepercayaan konsumen di pasar yang semakin kompetitif.

Kata kunci *E-Commerce; Perlindungan Data Pribadi; Transfer Data*

A. Pendahuluan

Dalam era globalisasi yang kita alami saat ini, konsep tata kelola kedaulatan suatu negara telah menjadi semakin terkait erat dengan perkembangan teknologi dan dunia digital.[1] Oleh karena itu, tidaklah cukup bagi sebuah negara hanya fokus pada pengawasan serta pengendalian wilayah fisik seperti daratan, perairan, dan udara semata. Sebaliknya, negara juga harus memberikan perhatian serius terhadap pengawasan serta pengendalian dalam ruang siber. Hal ini menjadi semakin penting karena perdagangan barang, jasa, dan aliran informasi, baik di dalam negeri maupun lintas negara, semuanya sangat bergantung pada aliran data digital yang semakin pesat.[2] Oleh karena itu, negara harus memiliki kemampuan untuk mengelola dan melindungi data digital guna menjaga kepentingan keamanan data digital negaranya.[3]

Saat ini, teknologi informasi memiliki dua sisi yang berlawanan, yakni memberikan kontribusi positif terhadap peningkatan kesejahteraan, kemajuan, dan peradaban manusia, tetapi juga dapat digunakan sebagai alat efektif untuk tindakan yang melanggar hukum.[4] Data pribadi, yang mencakup informasi sensitif seperti nama, alamat, nomor telepon, dan detail pribadi lainnya, telah menjadi bagian penting dalam kehidupan digital kita.[5] Penggunaannya meliputi pembelian *online*, media sosial, perbankan, dan sektor lainnya. Data ini bernilai tinggi, mempengaruhi cara kita berinteraksi *online*, dan juga menjadi sumber pendapatan bisnis.[6] Namun, kemudahan akses terhadap data pribadi ini juga membawa risiko serius terkait keamanan dan privasi.[7] Kehilangan atau penyalahgunaan data pribadi dapat berdampak merugikan pada individu dan masyarakat. Oleh karena itu, perlindungan data pribadi menjadi isu krusial yang memerlukan regulasi yang tepat di era global yang semakin terhubung ini.[8]

Selama beberapa tahun terakhir, perdagangan elektronik berkembang pesat di dunia, termasuk di Negara Indonesia. Sebagian besar aktivitas transaksi pembayaran dilakukan melalui Internet.[9] Berdasarkan penelitian oleh

---

[1] Sugeng. (2020). Hukum Telematika. Jakarta: Prenadamedia Group, p. 10
[2] Sidharta. (2000). Hukum Perlindungan Konsumen Indonesia. Jakarta: PT Grasindo, p. 7
[3] Gani T. A. (2023). Kedaulatan Data Digital untuk Integritas Bangsa. Syiah Kuala University Press, p. 3
[4] Ahmad M. Ramli. (2004). Cyber Law dan HAKI dalam Sistem Hukum Indonesia. Bandung: Refika Aditama, p. 11
[5] Dendi Sugiyono. (2008). Kamus Besar Bahasa Indonesia. Jakarta: Pusat Bahasa, p. 51
[6] Abdul Barkatullah Halim, dan Teguh Prasetyo. (2009). Bisnis E-commerce (Studi Sistem Keamanan Dan Hukum di Indonesia). Yogyakarta: Pustaka Pelajar, p. 13
[7] Danrivanto Budhijanto. (2017). Revolusi Cyberlaw Indonesia Pembaruan dan Revisi UU ITE 2016. Bandung: Refika Aditama, p. 15
[8] Rosadi S.D. (2015). Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional. Jakarta: Refika Aditama, p. 35
[9] Nugroho I.I., Pratiwi R., dan Zahro S.R.A., (2021), "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia", Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, Vol.1, No.2, p. 115

Communication and Information System Security Research Center (CISSReC), beberapa hasil menarik terungkap. Dari partisipan penelitian, 57% mengindikasikan keraguan terhadap keamanan SMS/*internet banking* di Indonesia. Di sisi lain, hanya 43% yang bersikap positif mengenai keamanan SMS/internet *banking* di Indonesia dengan keyakinan yang kuat. Data lain menunjukkan bahwa 66% responden merasa tidak percaya terhadap keamanan *e-commerc*e di Indonesia, sementara 34% tetap yakin pada keamanannya. Temuan lain dalam penelitian juga mengungkapkan bahwa 74% responden memiliki pemahaman dan kesadaran tentang potensi gangguan privasi yang mungkin timbul akibat penggunaan data pribadi dalam aplikasi atau layanan *online.* Dari angka tersebut, 13% menyatakan tidak merasa terganggu, sementara 13% lainnya mengaku kurang mengetahui dampaknya. Terkait pentingnya privasi, 81% responden meyakini perlindungan privasi penting. Meskipun demikian, hanya 4% yang tidak menganggap perlindungan privasi sebagai hal yang signifikan, dan 14% lainnya merasa ragu akan pentingnya perlindungan privasi. Secara keseluruhan, hasil penelitian CISSReC mencerminkan variasi pandangan di kalangan responden mengenai keamanan SMS/internet *banking*, *e-commerce*, serta kesadaran akan pentingnya privasi dan efeknya terhadap aktivitas *online*.[10]

Banyak negara telah mengembangkan hukum dan regulasi untuk menjaga privasi individu dan memastikan penggunaan data pribadi yang etis dalam kehidupan modern.[11] Di antara negara-negara yang berkomitmen terhadap masalah ini, Indonesia dan Malaysia menjadi subjek perbandingan menarik dalam konteks peraturan perlindungan data pribadi mereka yang unik dan berbeda.

Indonesia adalah salah satu negara di Asia Tenggara yang menghadapi tantangan dalam mengatur dan melindungi data pribadi dalam era digital ini. Perkembangan ekonomi digital, bisnis *online*, dan pertukaran data lintas negara telah memperumit isu-isu terkait privasi dan keamanan data pribadi. Oleh karena itu, penting untuk memahami dan membandingkan dengan negara lain agar menjadi evaluasi dan masukan untuk menghadapi isu perlindungan data pribadi dalam kerangka hukum mereka masing-masing.

Di antara sekian banyak kasus kebocoran data pribadi di Indonesia, salah satu yang paling mencuri perhatian publik adalah kasus kebocoran data yang dialami Tokopedia pada 20 Maret 2020, dimana hampir seluruh akunnya berhasil diretas oleh pihak peretas dan berhasil mengambil data-datanya.[12] Pelakunya, berhasil

---

[10] Fadhil, (2019), Riset: Kesadaran Keamanan Siber Di Masyarakat Masih Rendah, https://www.kominfo.go.id/content/detail/9992/riset-kesadaran-keamanan-siber-di-masyarakat-masih-rendah/0/sorotan_media, diakses pada 19 Oktober 2023.

[11] Mohammad Akbar Aldrin dan Alam. Sitti Nur. (2020). E-Commerce Dasar Teori dalam Bisnis Digital. Medan: Yayasan Kita Menulis, p. 21.

[12]Adhi Wicaksono, (2020), Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual, diakses pada 13 November 2023.

mencuri sekitar 91 juta data pengguna dan lebih dari 7 juta data *merchant* dari *platform* tersebut. Informasi yang berhasil diretas, seperti nama, alamat email, dan kata sandi pengguna, kemudian dijual dengan harga sekitar US$ 5.000 atau setara dengan Rp 74,5 juta dengan kurs Rp 14.900/US$. Tak lama setelah insiden tersebut, *platform* Bhinneka juga melaporkan kebocoran data yang serupa yang dilakukan oleh peretas yang sama.[13]

Kehadiran Undang-Undang Perlindungan Data Pribadi di Indonesia saat ini, yang telah mengatur berbagai jenis larangan dan sanksi terhadap pelanggaran terkait data pribadi, dapat menjadi dasar yang kokoh bagi Lembaga penegak hukum di masa depan untuk bertindak dan menjalankan penegakan hukum secara efisien.[14]

Namun, terdapat beberapa hal menarik yang dibahas dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) yaitu mengizinkan pengendali data pribadi untuk mentransfer data pribadi ke luar wilayah hukum Negara Republik Indonesia. Pasal ini tidak dengan tegas mengharuskan persetujuan pemilik data pribadi sebelum melakukan transfer data. Hal ini menciptakan kekhawatiran bahwa hak-hak pemilik data pribadi dapat diabaikan dan bertentangan dengan tujuan utama UU PDP, yaitu perlindungan data pribadi.

Oleh karena itu, data pribadi merupakan sebagai bagian esensial dari hak fundamental dan sumber nilai ekonomi, yang memerlukan perhatian serius terkait dengan transfer dan pengelolaannya.[15] Walaupun proses transfer data melibatkan izin, masih perlunya pembahasan seputar potensi risiko keamanan yang mungkin timbul. Meskipun hingga saat ini belum terdapat laporan kasus merugikan pemilik data, tetapi relevan untuk mengupayakan langkah-langkah pencegahan yang memadai. Penegakan aturan terkait transfer data harus menjadi prioritas, dan sanksi yang tegas perlu diterapkan sebagai pencegahan terhadap pelanggaran keamanan data. Pemerintah juga dapat mendorong transparansi dalam praktik pengelolaan data, memberikan pemilik data kontrol lebih besar terhadap informasi pribadi mereka.

Dalam konteks *e-commerce*, *platform-platform* tersebut perlu menerapkan langkah-langkah keamanan yang komprehensif, termasuk pelatihan karyawan, pemantauan sistem secara terus-menerus, dan peningkatan infrastruktur keamanan. Keterlibatan pihak ketiga untuk melakukan audit keamanan secara independen dapat menjadi mekanisme tambahan untuk mengevaluasi dan memverifikasi langkah-langkah keamanan yang diimplementasikan.

---

[13]Yosepha Pusparisa, (2020), Bocornya Puluhan Juta Data Pengguna E-Commerce Indonesia,https://databoks.katadata.co.id/datapublish/2020/05/12/bocornya-puluhan-juta-data-pengguna-e-commerce-indonesia, diakses pada 13 November 2023.

[14] Beni Kharisma Arrasuli dan Khairul Fahmi, (2019), "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol.9 No.2, p. 387

[15] Fathaniyah L., Makbul M., dan Makhrus M., (2023), "Urgensi Perlindungan Data Pribadi pada Transaksi E-Commerce Terhadap Pembangunan Ekonomi di Indonesia, Jurnal Hukum Ekonomi Syariah", Vol. 6, No. 2, p. 81

Dalam konteks ini, penelitian ini akan melakukan kajian mendalam terhadap regulasi perlindungan data pribadi di Indonesia. Penelitian ini bertujuan untuk memberikan wawasan yang lebih baik tentang cara kedua negara menghadapi tantangan terkait perlindungan data pribadi khususnya dalam transfer data dari *platform e-commerce* serta dampaknya pada masyarakat dan bisnis mereka. Dengan pemahaman yang lebih mendalam tentang isu ini, diharapkan penelitian dapat memberikan masukan bagi pemerintah serta pelaku bisnis dalam menghadapi era digital yang semakin kompleks.

B. Metode

Penelitian ini menggunakan metode hukum yuridis normatif sebagai pendekatan utama untuk menyelidiki permasalahan yang ada. Dalam rangka memberikan wawasan yang lebih komprehensif, penelitian ini mengadopsi dua pendekatan penelitian yaitu pendekatan perundang-undangan (*statute approach*) dan komparatif (*comparative approach*). Sumber data penelitian terdiri dari bahan hukum primer, sekunder, dan tersier, yang diperoleh melalui studi kepustakaan. Proses analisis data dilakukan dengan menggunakan metode deskriptif dan menerapkan logika deduktif

C. Hasil dan Pembahasan

1. Prinsip-prinsip Perlindungan Data Pribadi di Indonesia

Menurut data dari *We Are Social*, pada bulan Januari tahun 2023, pengguna internet di Indonesia mencapai 213 juta individu. Angka ini mewakili sekitar 77% dari total populasi Indonesia, yang berjumlah 276,4 juta orang pada awal tahun tersebut. Terjadi peningkatan sebesar 5,44% dalam jumlah pengguna internet di Indonesia dibandingkan dengan tahun sebelumnya (*year-on-year/yoy*). Pada bulan Januari 2022, jumlah pengguna internet di Indonesia hanya mencapai 202 juta orang.[16]

Sedangkan menurut Menurut data dari Statista Market Insights, pada tahun 2022, jumlah individu yang menggunakan *platform e-commerce* di Indonesia mencapai 178,94 juta orang. Angka ini menunjukkan peningkatan sebesar 12,79% jika dibandingkan dengan tahun sebelumnya, yang hanya mencapai 158,65 juta pengguna. Dengan melihat perkembangan ini, pengguna *e-commerce* di Indonesia terus mengalami pertumbuhan yang signifikan. Diperkirakan bahwa jumlah pengguna *e-commerce* akan mencapai 196,47 juta orang hingga akhir tahun 2023. Proyeksi ini menunjukkan bahwa tren peningkatan jumlah pengguna *e-commerce* diperkirakan akan berlanjut hingga empat tahun mendatang. Menurut Statista, pada

[16] Cindy Mutia Annur, (2023), Pengguna Internet di Indonesia Tembus 213 Juta Orang hingga Awal 2023, https://databoks.katadata.co.id/datapublish/2023/09/20/pengguna-internet-di-indonesia-tembus-213-juta-orang-hingga-awal-2023, diakses pada 28 Oktober 2023.

tahun 2027, jumlah pengguna *e-commerce* di Indonesia diperkirakan akan mencapai 244,67 juta individu.[17]

Prinsip-prinsip perlindungan data pribadi di Indonesia adalah dasar penting dalam mengatur dan melindungi informasi pribadi dalam era digital. Landasan utamanya adalah hak pemilik data untuk memiliki kendali atas data mereka. Ini berarti bahwa data pribadi hanya dapat dikumpulkan, diproses, atau disimpan setelah mendapatkan persetujuan pemilik data. Selain itu, transparansi dalam praktik pengumpulan data, tujuan yang terbatas, pengelolaan yang cermat tentang berapa lama data disimpan, serta perlindungan data yang kuat menjadi prinsip kunci dalam undang-undang perlindungan data pribadi. Hak pemilik data untuk mengakses, mengoreksi, atau bahkan menghapus data mereka juga menjadi prioritas.[18]

Prinsip perlindungan data pribadi berakar pada konsep privasi sebagai hak asasi manusia. Privasi mencakup hak untuk mengendalikan informasi pribadi dan telah diakui dalam hukum internasional. Namun, privasi bukan hak absolut, melainkan memiliki pengecualian yang berkaitan dengan kepentingan nasional dan publik. Konsep privasi telah berkembang seiring dengan inovasi teknologi komunikasi, yang juga memunculkan tantangan baru terkait pengawasan dan pengumpulan data yang dapat mengancam hak asasi manusia.[19]

Menurut pernyataan dari Kementerian Komunikasi dan Informatika, Undang-Undang Perlindungan Data Pribadi (UU PDP) akan mengawali periode baru dalam manajemen data pribadi di era digital di Indonesia.[20] Undang-Undang ini secara substansial terdiri dari 18 bab dan 78 pasal yang mengatur beragam aspek, tidak terbatas pada transfer data pribadi, sanksi administratif, lembaga penegak hukum, kerja sama internasional, partisipasi masyarakat, penyelesaian sengketa, hukum acara, larangan penggunaan data pribadi, ketentuan pidana, bersama dengan ketentuan peralihan dan penutup.

Prinsip perlindungan data pribadi di Indonesia tertuang dalam Pasal 16 ayat (2) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang berbunyi:

"(2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (l) dilakukan sesuai dengan prinsip Pelindungan Data Pribadi meliputi:

---

17 Ridwan Mustajab, (2023), Pengguna E-Commerce RI Diproyeksi Capai 196,47 Juta pada 2023, https://dataindonesia.id/digital/detail/pengguna-ecommerce-ri-diproyeksi-capai-19647-juta-pada-2023, diakses pada 28 Oktober 2023.

18 Rizal M.S., (2019), "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol.10, No.2, p. 221

19 Yuniarti S., (2019), "Perlindungan hukum data pribadi di Indonesia", Business Economic, Communication, and Social Sciences Journal (BECOSS), Vol.1, No.1, p. 150

20 Yovita, (2018), Indonesia sudah miliki aturan soal perlindungan Data Pribadi, https://www.kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-pribadi/0/sorotan_media, diakses pada 27 Oktober 2023.

a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;
b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
c. pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi;
d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan ;
e. pemrosesan Data Pribadi dilakukan dengan melindungi kemanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakkan, dan/atau penghilangan Data Pribadi;
f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Perlindungan Data Pribadi;
g. Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
h. Pemrosesan Data Pribadi dilakukansecara bertanggung jawab dan dapat dibuktikan secara jelas."

Peristiwa kegagalan dalam melindungi data pribadi yang sudah terjadi, sering kali pihak pengelola data pribadi baru menyadari tindakan yang tidak sah atau melanggar hukum terhadap data pribadi setelah perbuatan itu terjadi atau setelah berita tentang insiden tersebut menjadi dikenal luas. Situasi ini mengakibatkan kurangnya respons yang optimal dari pihak yang mengendalikan data pribadi. Terkadang, juga terjadi bahwa pengelola data pribadi menyangkal keberadaan tindakan yang tidak sah atau melanggar hukum terhadap data yang mereka tangani, meskipun ada bukti publik yang menunjukkan bahwa data pribadi telah diambil secara tidak sah atau melanggar hukum oleh pihak peretas. Kondisi semacam ini membuat pihak yang mengendalikan data pribadi memiliki sedikit opsi untuk mengambil tindakan guna melindungi data pribadi atau menjaga reputasi keamanan sistem perlindungan data yang mereka memiliki.[21]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi adalah regulasi yang mengatur perlindungan data pribadi secara spesifik di Indonesia. Undang-undang ini melindungi hak subjek data pribadi dengan mengatur aspek-aspek seperti informasi identitas yang jelas, dasar hukum penggunaan data, tujuan penggunaan data, serta akuntabilitas peminta data pribadi. Subjek data pribadi juga memiliki hak untuk menghentikan, atau menghapus data pribadi mereka, serta berhak untuk mengajukan gugatan dan menerima kompensasi atas pelanggaran pemrosesan data pribadi terhadap mereka.

[21] Rafifnafia Hertianto, (2021), "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia", Jurnal Kertha Patrika, Vol.43, No.1, p. 93-94

Selain itu, undang-undang ini fokus pada pencegahan kejahatan dengan metode yang tidak bersifat pidana, yang bertujuan mencegah pelanggaran pemrosesan data pribadi dan melindungi hak subjek data pribadi. Dengan Undang-Undnag Perlindungan Data Pribadi, pemerintah Indonesia berusaha memberikan perlindungan dan kepastian hukum kepada subjek data pribadi serta mengatasi akar masalah kejahatan dalam pengelolaan data pribadi.[22]

Perusahaan *e-commerce* menggunakan *platform marketplace* sebagai lokasi kegiatan bisnisnya, termasuk penggunaan data pribadi.[23] Menurut peraturan yang dijelaskan dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang pelaksanaan sistem dan transaksi elektronik, penyelenggaraan sistem elektronik dibagi menjadi dua wilayah, yakni lingkup publik dan privat:

a. Penyelenggara sistem elektronik lingkup publik merupakan pengoperasian sistem elektronik oleh badan pemerintah atau lembaga yang ditunjuk oleh badan pemerintah.
b. Penyelenggara sistem elektronik lingkup privat merupakan Pengelolaan sistem elektronik oleh individu, perusahaan, dan komunitas.[24]

Sebagai penyelenggara sistem elektronik, *e-commerce* memiliki tanggung jawab untuk menjalankan sistem elektronik dengan andal, keamanan, dan kebertanggungjawaban yang sesuai dengan prinsip-prinsip yang dijelaskan dalam Pasal 16 Ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Terdapat serangkaian kewajiban yang harus dipenuhi oleh penyelenggara *e-commerce*, yaitu sebagai berikut[25]:

a. Dapat memulihkan informasi elektronik dan/atau dokumen elektronik dengan integritas sesuai dengan jangka waktu retensi yang diatur dalam peraturan perundang-undangan;
b. Bertanggungjawab menjaga ketersediaan, keutuhan, otentikasi, kerahasiaan, dan aksesibilitas informasi elektronik dalam pengoperasian sistem elektronik;
c. Beroperasi sesuai dengan prosedur atau panduan yang berlaku dalam pengelolaan sistem elektronik;
d. Dilengkapi dengan panduan atau prosedur yang sesuai untuk pengelolaan sistem elektronik;

---

[22]Yudistira M., dan Ramadani R., (2023), "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO", UNES Law Review, Vol.5, No.4, p. 3812

[23] Pasal 1 ayat 1 Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi. Jakarta.

[24]Andrean W.Finaka, (2022), Apa Beda PSE Badan Publik dan Privat?, https://indonesiabaik.id/infografis/apa-beda-pse-badan-publik-dan-privat, diakses pada 27 Oktober 2023.

[25]Irawan, M. R., (2023). *Perlindungan Terhadap Data Pribadi Pengguna Aplikasi Perdagangan Elektronik*. Podomoro University.

e. Menyediakan panduan atau petunjuk yang diterbitkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang terlibat dalam pengoperasian sistem elektronik tersebut;
f. Memiliki mekanisme berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau panduan;
g. Memastikan bahwa sistem elektroniknya tidak digunakan untuk menyebarkan informasi elektronik dan/atau dokumen elektronik yang melanggar hukum sesuai dengan peraturan perundang-undangan;
h. Mematuhi prinsip perlindungan data pribadi;
i. Menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan atas permintaan individu yang bersangkutan;
j. Melakukan langkah-langkah keamanan untuk komponen sistem elektronik;
k. Menjaga kerahasiaan, integritas, otentikasi, aksesibilitas, ketersediaan, dan pelacakan informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan hukum yang berlaku;
l. Melindungi pengguna dan masyarakat umum dari kerugian yang disebabkan oleh sistem elektronik yang dijalankan;

Untuk memastikan perlindungan data pribadi yang efektif, penting untuk menetapkan hak dan kewajiban yang jelas bagi badan hukum yang mengelola data tersebut melalui undang-undang Perlindungan Data Pribadi. Pemrosesan data pribadi harus didasarkan pada dasar hukum yang sah, transparan, dan terbatas pada tujuan yang ditetapkan. Data pribadi harus dihapus atau dimusnahkan setelah periode pemrosesan berakhir. Namun, terdapat pengecualian berdasarkan peraturan instansi pengawas dan pengatur sektor yang relevan. Upaya lain untuk meningkatkan perlindungan data pribadi melibatkan penggunaan alat pemrosesan data dalam fasilitas publik dan peningkatan transparansi dalam lokasi pemasangan alat tersebut. Dengan mengatur hak dan kewajiban yang jelas, pemrosesan data yang tepat, dan tindakan perlindungan yang diperlukan, diharapkan perlindungan data pribadi dapat terjamin dengan baik.[26]

Tidak jauh berbeda dengan Indonesia, diperkirakan antara tahun 2023 dan 2027 jumlah pengguna *e-commerce* di Malaysia juga akan terus mengalami peningkatan, dengan penambahan sekitar 2,9 juta pengguna, yang setara dengan peningkatan sekitar 17,35%. Setelah mengalami peningkatan selama sepuluh tahun secara berturut-turut, perkiraan ini mencapai angka 19,64 juta pengguna dan mencapai puncak baru pada tahun 2027.[27]

---

[26] Wiwin Yulianingsih, dan Yuly Sari Kartika, (2023), "Kajian Yuridis Tindak Pidana Pemalsuan Identitas Data Diri Dalam Situs Bantuan Kartu Prakerja", Jurnal Rectum, Vol.5, No.2, p. 14

[27] Departemen Riset Statista, (2023), Jumlah pengguna e-commerce di Malaysia 2017-2027, https://www.statista.com/statistics/1351255/malaysia-number-of-e-commerce-users/, diakses pada 28 Oktober 2023.

Malaysia mbentukkan Undang-Undang Perlindungan Data Pribadi yang disebut *Personal Data Protection Act* 2010. Undang-undang ini memberikan perlindungan yang kuat terhadap hak privasi warga negaranya. Undang-undang data pribadi Malaysia telah berlaku sejak tahun 2013 dan mengatur prinsip-prinsip perlindungan data pribadi, hak pemilik data, pemindahan data, serta kewajiban penyimpan data.

Dengan diberlakukannya *Personal Data Protection Act* 2010, ini pemerintah Malaysia telah mengatur transfer data pribadi lintas negara, yang harus mematuhi ketentuan yang telah ditetapkan oleh Menteri Informasi, Kebudayaan, dan Komunikasi Malaysia, dan negara tujuan yang menerima data pribadi harus memberikan perlindungan setidaknya sebanding dengan yang diberikan oleh *Personal Data Protection Act* 2010 Malaysia.[28] Meski demikian, salah satu keprihatinan utama para konsumen *e-commerce* adalah tentang cara data pribadi mereka diperlakukan dan pentingnya menjaga privasi mereka saat beraktivitas *online*.[29]

Dengan demikian, Indonesia dan Malaysia sama-sama telah menerapkan kerangka kerja hukum untuk perlindungan data pribadi di era digital. Walaupun keduanya telah mengambil langkah untuk melindungi data pribadi individu, perbedaan mendasar menjadi jelas. Undang-undang Malaysia mengatur berbagai aspek perlindungan data pribadi dengan sangat terperinci, mencakup prinsip-prinsip yang spesifik, tata kelola yang ketat, dan mekanisme penegakan hukum yang jelas.

Di sisi lain, Indonesia baru-baru ini mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang merupakan langkah positif dalam menjaga privasi dan keamanan data. Namun, undang-undang ini masih memerlukan pengembangan lebih lanjut dalam hal rincian pelaksanaan dan penegakan hukum untuk mencapai tingkat perlindungan yang setara dengan negara seperti Malaysia.

Meskipun kedua negara telah mengakui pentingnya perlindungan data pribadi, Malaysia telah melangkah lebih jauh dengan undang-undang yang lebih matang dan komprehensif. Perbedaan ini mencerminkan tingkat kematangan dan kesiapan hukum masing-masing negara dalam menghadapi tantangan yang berkaitan dengan privasi dan data pribadi di era digital yang terus berkembang. Seiring waktu, Indonesia mungkin perlu terus memperkuat undang-undangnya dan meningkatkan kapasitas penegakan hukum untuk mengikuti perkembangan dunia digital yang semakin kompleks.

---

[28] Rizal M.S., (2019), "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol.10, No.2, p. 225

[29]Mira Mashor, (2022), Hukum dan Peraturan E-Commerce di Malaysia, https://www.mondaq.com/dodd-frank-consumer-protection-act/1244510/e-commerce-laws-and-regulations-in-malaysia, diakses pada 29 Oktober 2023.

2. Implikasi Regulasi Transfer Data Pribadi pada Perusahaan E-Commerce dalam prespektif Undang-Undang No. 27 Tahun 2022 Indonesia

Dalam era digital yang semakin maju, transfer data pribadi telah menjadi salah satu aspek krusial dalam ekosistem informasi global. Hal ini khususnya relevan dalam konteks perusahaan *e-commerce*. Data pribadi, yang mencakup informasi sensitif tentang individu, memiliki potensi besar dalam memberikan manfaat sosial, ekonomi, dan teknologi. Namun, potensi ini juga berdampingan dengan risiko terhadap privasi dan keamanan data, yang harus diatasi dengan cermat.[30]

Pemerintah Indonesia telah mengeluarkan serangkaian peraturan yang bertujuan untuk memastikan kelangsungan dan hubungan antara peraturan tersebut, dengan tujuan melindungi penggunaan dan penyebaran data pribadi dalam konteks *e-commerce*. Hal ini dimaksudkan untuk mengurangi potensi penyalahgunaan data pribadi. Pemerintah Indonesia telah mengenalkan perubahan signifikan dalam hal perlindungan data pribadi dengan menerbitkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang dikenal sebagai UU PDP. Undang-undang ini mulai berlaku pada tahun 2023, membawa perubahan substansial dalam regulasi data pribadi di Indonesia dan memberikan dasar hukum yang kuat untuk melindungi data individu serta mengatur transfer data pribadi di dalam dan di luar wilayah Indonesia. Ketentuan transfer data pribadi dalam Undang-Undang No. 27 Tahun 2022 tertuang dalam BAB VII Pasal 55-56.

Walaupun *e-commerce* menyediakan kenyamanan dalam bertransaksi, terdapat satu isu penting yang harus diperhatikan, yaitu privasi. Menurut Zheng Qin, yang disebutkan dalam buku *Introduction to E-Commerce*, saat melakukan transaksi online, kita perlu memberikan data pribadi kita. Selain itu, jejak aktivitas *online* kita dapat diawasi dan dicatat tanpa sepengetahuan kita, dan pihak yang mengumpulkan data ini kadang-kadang menjual informasi tersebut secara komersial kepada organisasi lain. Oleh karena itu, ketika kita terlibat dalam *e-commerce*, kita harus menyadari bahwa privasi kita bisa terancam.[31] Semua aktivitas ini berlangsung melalui jaringan komputer dan internet, yang pada gilirannya dapat menimbulkan permasalahan hukum baru terkait dengan cara informasi disampaikan, komunikasi, transaksi elektronik, dan juga bukti yang berkaitan dengan perbuatan hukum yang dilakukan melalui sistem elektronik.

E-commerce telah memacu pertumbuhan ekonomi dengan cepat. Oleh karena itu, untuk terus meningkatkan pendapatan dalam sektor digital, tidak hanya perlu memperhatikan masalah perpajakan, ketersediaan barang dan jasa melalui *platform* digital, serta program digitalisasi untuk UMKM. Keamanan data pribadi juga harus menjadi perhatian utama, mengingat bahwa kebocoran data pribadi bisa terjadi karena kelemahan dalam sistem pengelolaan data pribadi atau penyelenggara

---

[30] Yuniarti S., (2019), "Perlindungan hukum data pribadi di Indonesia", Business Economic, Communication, and Social Sciences Journal (BECOSS), Vol.1, No.1, p. 149

[31] Zheng Qin. (2009). Introduction to E-Commerce. Beijing: Tsinghua University, p. 193-194

sistem elektronik dalam melindungi sistem mereka, dan juga karena kemungkinan serangan oleh para peretas.[32]

Kebocoran data pribadi memiliki potensi dampak negatif yang signifikan terhadap pembangunan ekonomi nasional, dengan beberapa implikasi yang mencakup:

a. Menurunnya Kepercayaan Konsumen: Kebocoran data pribadi dapat mengakibatkan penurunan kepercayaan konsumen terhadap *platform* atau perusahaan yang terlibat. Ini dapat menghambat pertumbuhan bisnis dan mengurangi jumlah transaksi online.
b. Ancaman terhadap Privasi Individu: Pelanggaran data pribadi mengancam privasi individu, yang merupakan hak asasi manusia yang penting. Hal ini dapat merusak citra perusahaan dan menyebabkan masalah hukum.
c. Gangguan pada Kegiatan Bisnis: Ketika data pribadi terungkap, hal ini dapat mengakibatkan gangguan pada operasi bisnis, seperti tuntutan hukum, perbaikan keamanan, dan biaya pemulihan data yang signifikan.
d. Penurunan Investasi Asing: Kondisi keamanan data yang buruk dapat mengurangi minat investor asing untuk beroperasi di negara tersebut. Hal ini dapat menghambat pertumbuhan ekonomi dan investasi asing yang dibutuhkan untuk pengembangan industri.

Perusahaan *e-commerce*, sebagai badan hukum yang beroperasi, termasuk dalam kategori pengendali data pribadi yang harus mematuhi peraturan perlindungan data pribadi yang diatur dalam UU PDP. Ada beberapa prinsip yang harus diikuti oleh pengendali data pribadi saat mereka melakukan pemrosesan data pribadi, antara lain[33]:

a. Data pribadi harus dikumpulkan dengan cara yang spesifik, terbatas, sah secara hukum, dan transparan;
b. Data pribadi harus diolah sesuai dengan tujuan yang ditetapkan;
c. Hak-hak subjek data pribadi harus dijamin saat pengolahan data;
d. Data pribadi harus dikelola dengan akurat, lengkap, tidak menyesatkan, selalu diperbarui, dan dapat dipertanggungjawabkan;
e. Data pribadi harus dilindungi dari akses, pengungkapan, perubahan, penyalahgunaan, kerusakan, atau hilangnya data yang tidak sah;
f. Tujuan dan aktivitas pemrosesan data pribadi, serta potensi risiko yang terkait dengan pelindungan data pribadi, harus dijelaskan kepada subjek data;
g. Data pribadi harus dihapus setelah periode retensi berakhir, kecuali ada ketentuan lain dalam peraturan yang berlaku;

---

[32] Orinaldi M., (2020), "Peran E-commerce dalam Meningkatkan Resiliensi Bisnis diera Pandemi", ILTIZAM Journal of Shariah Economics Research. Vol.4, No.2, p. 41

[33] Pasal 16 Ayat 2 Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi. Jakarta.

h. Pengolahan data pribadi harus dilakukan secara bertanggung jawab dan dapat dibuktikan dengan jelas.

Berdasarkan peraturan di atas, pada prinsipnya, perusahaan *e-commerce* memiliki tanggung jawab untuk mencegah kebocoran data pribadi dengan menjaga keamanan data tersebut, sehingga terhindar dari akses yang tidak sah, pengungkapan, perubahan yang tidak sah, penyalahgunaan, kerusakan, dan kehilangan data pribadi. Jika terjadi kebocoran data pribadi, perusahaan *e-commerce* terkait harus memberikan pemberitahuan tertulis kepada pengguna yang mengelola data pribadi dalam waktu paling lama 3x24 jam.[34]

Pemberitahuan tersebut harus mencakup informasi tentang data pribadi yang terungkap, waktu dan metode kebocoran data pribadi, serta langkah-langkah yang diambil untuk menangani dan memulihkan kebocoran data pribadi. Jika kebocoran data pribadi tersebut mencapai tingkat yang mengganggu layanan publik dan/atau berdampak serius pada kepentingan masyarakat, maka perusahaan *e-commerce* harus mengumumkan kebocoran tersebut kepada masyarakat.[35]

Dengan berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, muncul solusi yang sangat relevan untuk menangani masalah yang semakin umum, yaitu kebocoran data pribadi. Undang-undang ini, yang didasarkan pada Pasal 55-56, menggariskan dengan jelas kewajiban pengendali data untuk melakukan melakukan mekanisme transfer data yang cermat dan menjaga keamanan data pribadi konsumen. Artinya, perusahaan yang mengumpulkan dan mengelola data pribadi harus secara aktif melindungi informasi sensitif tersebut.[36]

Sebagai aspek penting, jika terjadi kebocoran data yang disebabkan oleh pihak ketiga, tanggung jawab atas keamanan data tetap ada pada pengendali data. Ini adalah langkah yang penting dalam menjaga integritas dan kepercayaan dalam ekosistem digital. Dalam konteks ini, Undang-Undang Perlindungan Data Pribadi menghadirkan kerangka hukum yang kuat untuk melindungi hak dan privasi individu serta menegakkan standar keamanan data.[37]

Undang-undang ini juga menyatakan bahwa jika terjadi kegagalan dalam menjaga data pribadi, pengendali data akan dikenakan sanksi administratif. Ini memberikan insentif yang kuat bagi perusahaan yang terlibat untuk meningkatkan langkah-langkah keamanan dan pengawasan mereka, serta mendorong perubahan dalam budaya perlindungan data.[38]

---

[34] Pasal 46 Ayat 1 Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi. Jakarta.
[35] Pasal 46 Ayat 2 Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi. Jakarta.
[36] Nafiatul Munawaroh, (2022), Tanggung Jawab E-Commerce atas Kebocoran Data Pribadi, https://www.hukumonline.com/klinik/a/tanggung-jawab-ie-commerce-i-atas-kebocoran-data-pribadi-lt63638331d18f0/, diakses pada 29 Oktober 2023.
[37] Yudistira M., dan Ramadani R., (2023), "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO", UNES Law Review, Vol.5, No.4, p. 3922
[38] Gillang Achmad R., dan Toto Tohir S, (2023), "Perlindungan Hukum atas Kebocoran Data Pribadi

Selain itu, berdasarkan penjelasan dari Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, Semuel Abrijani Pangerapan, yang mewakili Pemerintah dalam sidang keempat Perkara Nomor 108/PUU-XX/2022 dan Perkara Nomor 110/PUU-XX/2022, disampaikan bahwa Pasal 2 ayat (2) UU PDP mengenai "kegiatan pribadi" atau "kegiatan rumah tangga" memiliki makna bahwa kegiatan tersebut terjadi dalam lingkup privat, bersifat personal, nonkomersial, dan nonprofesional. Pengecualian yang diatur dalam pasal tersebut dianggap sebagai upaya untuk melindungi hak asasi manusia, khususnya dalam menjaga hak privasi setiap individu, sebagaimana yang diamanatkan oleh Pasal 28G ayat (1) UUD 1945.[39]

Oleh karena itu, Undang-Undang Perlindungan Data Pribadi telah menjadi payung hukum yang sangat relevan baik dalam lingkup privat, bersifat personal, nonkomersial, dan nonprofesional di era di mana kebocoran data pribadi semakin sering terjadi. Dengan mengatur standar dan tindakan yang harus diambil dalam mengelola data pribadi, undang-undang ini membantu menjaga kepercayaan konsumen, mendukung pertumbuhan *e-commerce*, dan memberikan landasan yang kuat untuk melindungi privasi individu di era digital yang semakin canggih.

Regulasi transfer data pribadi pada perusahaan *e-commerce* menjadi fondasi yang tidak dapat diabaikan. Seperti negara-negara lainnya, Indonesia berusaha untuk menjaga keseimbangan antara inovasi bisnis dan perlindungan privasi individu. Implikasi hukum yang Penulis bahas di atas adalah bagian dari upaya untuk mencapai tujuan tersebut. Perusahaan *e-commerce* di Indonesia harus secara aktif mematuhi peraturan ini, tidak hanya untuk mematuhi hukum, tetapi juga untuk mempertahankan kepercayaan pelanggan, yang menjadi unsur kunci dalam lingkungan bisnis digital yang semakin kompetitif dan kompleks.

D. Simpulan

Berdasarkan pembahasan penelitian di atas, dapat disimpulkan bahwa Penelitian ini mengambil fokus pada prinsip-prinsip perlindungan data pribadi di Indonesia, mengingat pertumbuhan pesat pengguna internet dan e-commerce di Indonesia. Kesenjangan dalam respons terhadap pelanggaran data pribadi dan pengelolaan data yang kurang optimal telah menjadi isu menarik. Kondisi ini memerlukan perhatian serius, mengingat peristiwa kegagalan seringkali baru disadari setelah menjadi publik. Undang-Undang Perlindungan Data Pribadi memberikan landasan yang kuat, tetapi keberhasilannya juga bergantung pada kapasitas penegakan hukum dan kesadaran penuh dari pihak yang mengelola data pribadi. Prinsip-prinsip tersebut melibatkan hak pemilik data untuk mengendalikan

Konsumen PT PLN Dihubungkan dengan Hak Atas Keamanan Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi", Law Studies, Vol.3, No.1, p. 228-230

[39] Sri Pujianti, (2023), Pemerintah: UU Perlindungan Data Pribadi Beri Perlindungan Hukum, https://www.mkri.id/index.php?page=web.Berita&id=18915, diakses pada 10 Desember 2023.

data mereka, transparansi dalam praktik pengumpulan data, tujuan yang terbatas, manajemen yang cermat terkait masa retensi data, serta perlindungan data yang kuat. Perlindungan data pribadi di Malaysia lebih mencerminkan pendekatan yang lebih matang, yang terlihat dari Undang-Undang Personal Data Protection Act 2010. Meskipun Indonesia telah melangkah dengan baik dengan Undang-Undang Perlindungan Data Pribadi, perbedaan mendasar dengan regulasi Malaysia menjadi jelas. Malaysia telah merumuskan undang-undang yang sangat rinci dan komprehensif, menunjukkan kematangan hukum yang lebih tinggi. Ketika mengevaluasi implikasi regulasi transfer data pribadi pada perusahaan e-commerce di Indonesia, fokus utamanya adalah pada Undang-Undang No. 27 Tahun 2022. Hal ini menjadi landasan untuk mengatasi risiko privasi dan keamanan data dalam ekosistem digital. Perusahaan e-commerce memiliki tanggung jawab besar dalam menjaga keamanan data pribadi konsumen dan mematuhi prinsip-prinsip yang diatur oleh UU PDP.

Tidak hanya itu, kebocoran data pribadi dapat memiliki dampak negatif signifikan, termasuk penurunan kepercayaan konsumen, ancaman terhadap privasi individu, gangguan pada kegiatan bisnis, dan bahkan penurunan investasi asing. UU PDP memberikan solusi yang relevan, memberikan payung hukum yang kuat untuk melindungi hak dan privasi individu serta menegakkan standar keamanan data. Implikasi hukum tersebut diakui sebagai langkah positif dalam menjaga integritas dan kepercayaan dalam ekosistem digital yang semakin kompleks. Oleh karena itu, perusahaan e-commerce di Indonesia perlu tidak hanya mematuhi peraturan ini untuk menjaga kepatuhan hukum, tetapi juga untuk mempertahankan kepercayaan pelanggan dalam lingkungan bisnis digital yang semakin kompetitif

E. Referensi

Abdul Barkatullah Halim, dan Teguh Prasetyo. (2009). Bisnis E-commerce (Studi Sistem Keamanan Dan Hukum di Indonesia). Yogyakarta: Pustaka Pelajar

Ahmad M. Ramli. (2004). Cyber Law dan HAKI dalam Sistem Hukum Indonesia. Bandung: Refika Aditama

Beni Kharisma Arrasuli dan Khairul Fahmi, (2019), "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol.9 No.2, p. 387

Danrivanto Budhijanto. (2017). Revolusi Cyberlaw Indonesia Pembaruan dan Revisi UU ITE 2016. Bandung: Refika Aditama

Dendi Sugiyono. (2008). Kamus Besar Bahasa Indonesia. Jakarta: Pusat Bahasa

Fathaniyah L., Makbul M., dan Makhrus M., (2023), "Urgensi Perlindungan Data Pribadi pada Transaksi E-Commerce Terhadap Pembangunan Ekonomi di Indonesia, Jurnal Hukum Ekonomi Syariah", Vol. 6, No. 2, p. 81

Gillang Achmad R., dan Toto Tohir S, (2023), "Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan dengan Hak Atas Keamanan Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi", Law Studies, Vol.3, No.1, p. 228-230

Gani T. A. (2023). Kedaulatan Data Digital untuk Integritas Bangsa. Syiah Kuala University Press

Irawan, M. R., (2023). Perlindungan Terhadap Data Pribadi Pengguna Aplikasi Perdagangan Elektronik. Podomoro University

Nugroho I.I., Pratiwi R., dan Zahro S.R.A., (2021), "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia", Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, Vol.1, No.2, p. 115

Mohammad Akbar Aldrin dan Alam. Sitti Nur. (2020). E-Commerce Dasar Teori dalam Bisnis Digital. Medan: Yayasan Kita Menulis

Rosadi S.D. (2015). Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional. Jakarta: Refika Aditama

Orinaldi M., (2020), "Peran E-commerce dalam Meningkatkan Resiliensi Bisnis diera Pandemi", ILTIZAM Journal of Shariah Economics Research. Vol.4, No.2, p. 41

Rafifnafia Hertianto, (2021), "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia", Jurnal Kertha Patrika, Vol.43, No.1, p. 93-94

Rizal M.S., (2019), "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol.10, No.2, p. 221

Sidharta. (2000). Hukum Perlindungan Konsumen Indonesia. Jakarta: PT Grasindo

Sugeng. (2020). Hukum Telematika. Jakarta: Prenadamedia Group

Wiwin Yulianingsih, dan Yuly Sari Kartika, (2023), "Kajian Yuridis Tindak Pidana Pemalsuan Identitas Data Diri Dalam Situs Bantuan Kartu Prakerja", Jurnal Rectum, Vol.5, No.2, p. 14

Yudistira M., dan Ramadani R., (2023), "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO", UNES Law Review, Vol.5, No.4, p. 3812

Yuniarti S., (2019), "Perlindungan hukum data pribadi di Indonesia", Business Economic, Communication, and Social Sciences Journal (BECOSS), Vol.1, No.1, p. 150

Zheng Qin. (2009). Introduction to E-Commerce. Beijing: Tsinghua University *ADIL: Jurnal Hukum* 4, no. 1 (2015). https://doi.org/10.33476/ajl.v4i1.28.