BAB I

PENDAHULUAN

A. Latar Belakang Masalah

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

[1] Sugeng, 2020, *Hukum Telematika*, Jakarta, Prenadamedia Group, hlm. 10
[2] Sidharta, 2000, *Hukum Perlindungan Konsumen Indonesia*, Jakarta, PT Grasindo, hlm. 7
[3] Gani T. A., 2023, *Kedaulatan Data Digital untuk Integritas Bangsa*, Syiah Kuala University Press, hlm. 3
[4] Ahmad M. Ramli, 2004, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, Bandung, Refika Aditama, hlm. 11

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 Indonesia dan Malaysia. Sebagian besar aktivitas transaksi pembayaran dilakukan melalui Internet.[9] Berdasarkan penelitian oleh *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

[5] Dendi Sugiyono, 2008, *Kamus Besar Bahasa Indonesia,* Jakarta, Pusat Bahasa, hlm. 51
[6] Abdul Barkatullah Halim, dan Teguh Prasetyo, 2009, *Bisnis E-commerce (Studi Sistem Keamanan Dan Hukum di Indonesia)*, Yogyakarta, Pustaka Pelajar, hlm. 13
[7] Danrivanto Budhijanto, 2017, *Revolusi Cyberlaw Indonesia Pembaruan dan Revisi UU ITE 2016*, Bandung, Refika Aditama, hlm. 15
[8] Rosadi S.D, 2015, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Jakarta, Refika Aditama, hlm. 35
[9] Nugroho I.I., Pratiwi R., dan Zahro S.R.A., "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia", *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, Vol.1, No.2, (Desember, 2021), hlm. 115

menunjukkan bahwa 66% responden merasa tidak percaya terhadap keamanan *e-commer*ce 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]

Selain itu, Malaysia juga dapat menembus presentase pengguna *e-commerce* yang signifikan, yaitu mencapai angka sebesar 34,7%, menunjukkan pertumbuhan yang cukup besar dalam adopsi perdagangan elektronik di negara tersebut. Peningkatan signifikan ini mencerminkan pergeseran kuat menuju tren belanja *online* di Malaysia, dengan masyarakat semakin memanfaatkan *platform-platform e-commerce* untuk memenuhi kebutuhan mereka. Dengan presentase tersebut dapat disimpulkan bahwa *e-commerce* tidak hanya menjadi

[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, 09:00)

fenomena tetapi juga telah menjadi bagian integral dari pola konsumsi masyarakat Malaysia, menciptakan dampak positif dalam transformasi ekonomi digital di negara tersebut.[11]

Banyak negara telah mengembangkan hukum dan regulasi untuk menjaga privasi individu dan memastikan penggunaan data pribadi yang etis dalam kehidupan modern.[12] 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 dan Malaysia adalah dua negara di Asia Tenggara yang sama-sama menghadapi tantangan dalam mengatur dan melindungi data pribadi dalam era digital ini. Perkembangan ekonomi digital, bisnis *online*, dan pertukaran data lintas batas negara telah memperumit isu-isu terkait privasi dan keamanan data pribadi. Oleh karena itu, penting untuk memahami dan membandingkan bagaimana kedua negara ini 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

[11] Cindy Mutia Annur, 2022, *Daftar Negara Paling Sering Belanja Online, Indonesia Peringkat ke-5,* https://databoks.katadata.co.id/datapublish/2022/02/14/daftar-negara-paling-sering-belanja-online-indonesia-peringkat-ke-5, (diakses pada 10 Desember 2023, 08:15)
[12] Mohammad Akbar Aldrin dan Alam. Sitti Nur, 2020, *E-Commerce Dasar Teori dalam Bisnis Digital*, Medan, Yayasan Kita Menulis, hlm. 21.

berhasil diretas oleh pihak peretas dan berhasil mengambil data-datanya.[13] Pelakunya, berhasil 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.[14]

Pada 25 Oktober 2022 Sejumlah 2,6 juta pengguna Carousell dari Malaysia dan Singapura telah mengalami pelanggaran keamanan data pada *platform* penjualan barang bekas *online* yang terkenal. Informasi yang dicuri, termasuk tanggal pembuatan akun, nama pengguna, nama lengkap, alamat email, nomor telepon, dan data lainnya, dijual secara daring dengan harga US$1.000 (RM4.412). Hasil dari investigasi menunjukkan adanya kelemahan dalam proses migrasi sistem yang digunakan oleh pihak ketiga, yang memungkinkan mereka untuk mendapatkan akses tidak sah ke *database* perusahaan.[15]

Dua kasus diatas telah menjadi sorotan utama dalam perbincangan masyarakat serta menggarisbawahi eskalasi masalah keamanan data yang semakin meresahkan di era digital ini. Kasus semacam ini mengingatkan kita tentang urgensi perlindungan

[13]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, 08:00)

[14]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, 08:15)

[15] Khairul Haqiem, 2023, *Pelanggaran Data Berulang di Malaysia - Ketidaktahuan atau Hanya Lemahnya Penegakan*, https://cybersecurityasean.com/daily-news/recurring-data-breaches-malaysia-plain-ignorance-or-just-weak-enforcement, (diakses pada 13 November 2023, 09:00)

data pribadi dan betapa pentingnya upaya pencegahan dan penegakan hukum yang lebih ketat dalam menangani ancaman keamanan siber.

Di Indonesia, regulasi perlindungan data pribadi diatur oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.[16] Undang-undang ini adalah langkah signifikan dalam upaya memberikan perlindungan yang lebih kuat terhadap informasi pribadi individu di Indonesia. Sementara itu, di Malaysia, undang-undang yang relevan adalah Undang-Undang perlindungan data pribadi Malaysia atau *Personal Data Protection Act* 2010.[17] PDPA 2010 merupakan peraturan yang penting untuk menjaga keamanan data pribadi di Malaysia, dan juga mengikuti tren global dalam memberikan perlindungan yang memadai terhadap informasi pribadi dalam era digital yang semakin maju. Kedua undang-undang ini mencerminkan kesadaran akan pentingnya mengatur dan melindungi data pribadi di dunia yang semakin terhubung dan serba digital saat ini.

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.[18]

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

[16] Manurung E.A.P., dan Thalib E.F., "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022", *Jurnal Hukum Saraswati (JHS)*, Vol. 4, No.2, (Januari, 2022), hlm. 144
[17] Ghani F.A., Razali N.A., dan Shabri S.M., "Akta Perlindungan Data Peribadi 2010: Satu Tinjaun", *Jurnal Dunia Pengurusan*, Vol.3, No.1, (Maret, 2021), hlm. 3
[18] Beni Kharisma Arrasuli dan Khairul Fahmi, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum*, Vol.9 No.2, (Juli, 2019), hlm. 387

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.

Permasalahan lain yaitu ketidakpastian hukum terkait perlindungan data pribadi karena tidak ada hukum yang secara eksplisit mengatur penanganan masalah hukum terkait penyalahgunaan data pribadi. Pengaturan perlindungan data pribadi tersebar di berbagai hukum dan peraturan yang ada, dan hal ini menciptakan kebingungan dan ketidakpastian dalam penegakan hukum di bidang ini.

Sedangkan Undang-Undang *the Personal Data Protection Act* 2010 Malaysia telah meningkatkan tingkat keamanan data pribadi pengguna internet di Malaysia. PDPA Malaysia juga mengatur bahwa transfer data pribadi ke luar Malaysia hanya diperbolehkan dengan izin dari Menteri Informasi, Kebudayaan, dan Komunikasi, serta dengan jaminan bahwa negara atau wilayah penerima data pribadi menyediakan tingkat perlindungan data pribadi yang setara dengan yang diberikan oleh PDPA Malaysia.[19]

Implementasi ketentuan-ketentuan ini telah memberikan kepastian hukum yang signifikan terkait dengan keamanan data pribadi warga Malaysia.[20] Warga negara Malaysia dapat merasa lebih tenang karena data pribadi mereka dilindungi dengan ketat. Dengan demikian, PDPA Malaysia telah berperan penting dalam

[19] Nadiah Tsamara, "Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara", *Jurnal Suara Hukum*. Vol.3 No.1, (Maret, 2021), hlm. 72-73
[20] Aini Sulaiman, Rohana Jani, dan Shamshul Bahri, 2001, *The Development of E-Commerce in Malaysia,* Kuala Lumpur, University of Malaya, hlm. 15

melindungi privasi dan keamanan data pribadi dalam era digital yang semakin kompleks ini.

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.[21] 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.

Berdasarkan uraian diatas, maka peneliti tertarik untuk melakukan penelitian tentang regulasi perlindungan data pribadi antara Indonesia dan

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

Malaysia. Karena antara kedua negara ini memiliki perbedaan mendasar dalam pendekatan hukum dan regulasi. Perbedaan ini mencakup pengaturan perizinan pemrosesan data pribadi, hak individu terkait data pribadi, serta tanggung jawab pemilik data antara Indonesia dan Malaysia.

Selain itu, dampak dari perbedaan-perbedaan ini juga dapat dirasakan oleh bisnis dan individu yang terlibat dalam pengelolaan dan pengolahan data pribadi di kedua negara. Hal ini dapat melibatkan masalah seperti biaya kepatuhan, risiko hukum, dan perlindungan hak privasi individu.

Dalam konteks ini, penelitian ini akan melakukan kajian mendalam terhadap regulasi perlindungan data pribadi di Indonesia dan Malaysia. Dengan menganalisis perbedaan-perbedaan, 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 pembuat kebijakan serta pelaku bisnis dalam menghadapi era digital yang semakin kompleks.

B. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, dalam penelitian ini akan membahas mengenai:

1. Apa perbedaan utama yang terdapat dalam pendekatan hukum Indonesia dan Malaysia terhadap perlindungan data pribadi, khususnya pada transfer data pribadi oleh perusahaan *e-commerce*?

2. Bagaimana implikasi dari transfer data pribadi oleh *e-commerce* menurut kajian Undang-Undang No. 27 Tahun 2022 Indonesia dan *Personal Data Protection Act* 2010 Malaysia?

C. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini meliputi hal-hal sebagai berikut:

1. Untuk menganalisis perbedaan utama yang terdapat dalam pendekatan hukum Indonesia dan Malaysia terhadap perlindungan data pribadi, khususnya pada transfer data pribadi oleh perusahaan *e-commerce.*
2. Untuk menganalisis dan memahami implikasi dari transfer data pribadi yang dilakukan oleh perusahaan *e-commerce*, dengan fokus pada peraturan yang tertuang dalam Undang-Undang No. 27 Tahun 2022 di Indonesia dan *Personal Data Protection Act* 2010 Malaysia.

D. Manfaat Penelitian

Adapun manfaat yang ingin dicapai dalam penelitian ini mencakup hal-hal sebagai berikut:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat memberikan kontribusi ilmiah yang berharga dan menjadi acuan yang berguna bagi mahasiswa, pengajar, serta praktisi di bidang hukum dalam hal penulisan karya ilmiah yang berkaitan dengan peraturan perlindungan data pribadi, terutama dalam konteks transfer data pribadi khususnya pada *e-commerce* di Negara Indonesia dan Malaysia.

2. Manfaat Praktis

   a. Pemerintah: Informasi tentang perbedaan dalam regulasi perlindungan data pribadi dapat memberikan wawasan kepada pembuat kebijakan di kedua negara yaitu Indonesia dan Malaysia. Keduanya dapat menggunakan penelitian ini sebagai dasar untuk memperbarui atau memperbaiki regulasi yang ada.

   b. Kalangan Pembisnis: Bisnis yang beroperasi di kedua negara yaitu Indonesia dan Malaysia dapat menggunakan informasi ini untuk memahami kewajiban mereka terkait data pribadi. Ini membantu mereka mematuhi hukum yang berlaku dan mengurangi risiko hukum.

   c. *E-Commerce*: Penelitian ini akan membantu meningkatkan keamanan data pribadi yang ditransfer melalui *platform e-commerce* dengan mengidentifikasi celah keamanan yang mungkin ada dalam regulasi dan memberikan rekomendasi perbaikan. Hal ini akan memberikan perlindungan yang lebih kuat terhadap informasi pribadi pengguna dalam aktivitas *e-commerce*, mendorong kepercayaan konsumen, dan meminimalkan risiko penyalahgunaan data.

   d. Masyarakat: Masyarakat dapat memahami hak privasi mereka dan cara melindungi data pribadi mereka dalam lingkungan digital yang semakin kompleks. Mereka dapat lebih waspada terhadap risiko penyalahgunaan data pribadi.

   e. Kolaborasi Internasional: Penelitian ini dapat membuka pintu untuk kolaborasi lebih lanjut antara Indonesia dan Malaysia, serta negara

lain, dalam mengatasi tantangan perlindungan data pribadi di era global.

f. Pendidikan: Informasi ini dapat digunakan dalam program pendidikan dan pelatihan untuk menghasilkan para profesional yang memahami isu-isu perlindungan data pribadi dan dapat membantu bisnis dan pemerintah untuk mematuhi regulasi yang berlaku.