

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

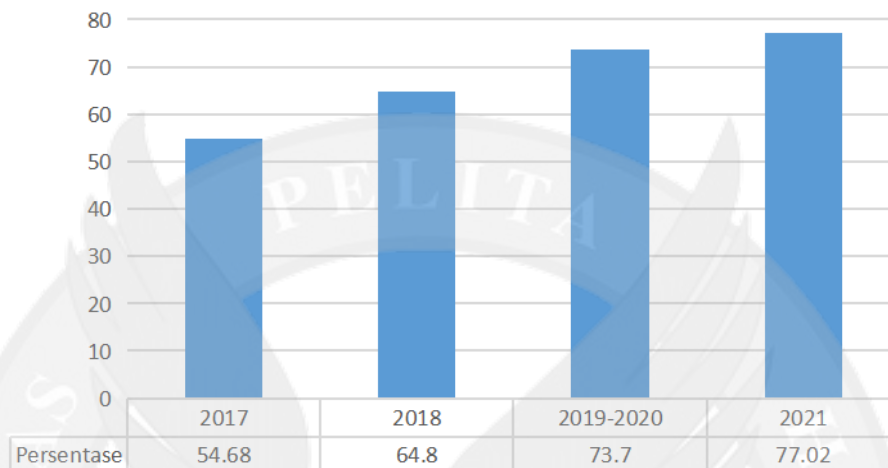
Dalam beberapa dekade terakhir, teknologi mengalami perkembangan yang cukup pesat. Perkembangan teknologi ini telah mempengaruhi hampir seluruh aspek kehidupan masyarakat. Industri perdagangan (*e-commerce*), keuangan, kesehatan, pariwisata, hingga pemerintahan ikut merasakan perkembangan teknologi dan melakukan interaksi dalam *platform digital*. Teknologi tidak hanya berperan untuk memperoleh informasi atau media komunikasi, namun juga mendorong pertumbuhan ekonomi di era *digital*.

Akselerasi ekonomi *digital* dipercaya mampu mendorong pertumbuhan ekonomi Indonesia dengan dukungan beberapa faktor. Pertama, berdasarkan sensus penduduk 2020, Indonesia memiliki pangsa pasar yang besar dengan jumlah penduduk sebanyak 270.203.917 jiwa.¹ Kedua, penetrasi penggunaan internet di Indonesia mengalami peningkatan sebanyak 22,34% dalam waktu lima tahun terakhir dengan rincian berikut dapat dilihat pada Gambar 1.1.

Menurut Menteri Koordinator bidang Perekonomian RI, Airlangga, dalam Siaran Pers HM.4.6/179/SET.M.EKON.3/4/2022, pada tahun 2021 nilai transaksi *e-commerce* di Indonesia mencapai US\$53 miliar dan diprediksi akan

¹ Badan Pusat Statistik, “Jumlah dan Distribusi Penduduk”, <https://sensus.bps.go.id/main/index/sp2020#:~:text=Jumlah%20penduduk%20Indonesia%20pada%20tahun,133.542.018%20untuk%20penduduk%20perempuan>, diakses 25 Februari 2023, pukul 22:00.

meningkat sampai US\$104 miliar pada tahun 2025 dengan level pertumbuhan 18%.² Data tersebut menunjukkan kontribusi terbesar bagi ekonomi *digital* Indonesia datang dari transaksi *e-commerce*.



Gambar 1.1. Persentase Penetrasi Pengguna Internet pada Tahun 2017-2021³

Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 1 Ayat 2, “transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.”⁴ Berdasarkan pengertian ini, transaksi elektronik merupakan aktivitas penyebaran, penjualan, pembelian, pemasaran produk

² Kementerian Koordinator Bidang Perekonomian Republik Indonesia, “Akselerasi Ekonomi *Digital* pada *e-commerce* dan *Online Travel* Menjadi Salah Satu Strategi Efektif Mendorong Kinerja Perekonomian Nasional”, <https://www.ekon.go.id/publikasi/detail/3978/akselerasi-ekonomi-digital-pada-e-commerce-dan-online-travel-menjadi-salah-satu-strategi-efektif-mendorong-kinerja-perekonomian-nasional>, diakses 25 Februari 2023, pukul 22:10.

³ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Penetrasi & Perilaku Pengguna Internet Indonesia 2017, 2018, 2019-2020 (Q2), 2022.

⁴ Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

(barang dan jasa), dengan memanfaatkan jaringan internet. Meskipun konsumen dan penjual tidak bertemu langsung secara tatap muka, transaksi tetap berjalan dengan dilakukan secara elektronik.

Ditinjau dari segi praktis, menurut Turban dkk., transaksi *e-commerce* dapat didefinisikan sebagai berikut:

“Sebuah aktivitas menjual dan membeli secara elektronik yang berhubungan antara pelaku usaha dan konsumen (*business-to-consumer* B2C) dan antara sesama pelaku usaha (*business-to-business* B2B)”⁵

Berdasarkan penjelasan di atas, transaksi *e-commerce* adalah sebuah kegiatan jual beli antar sesama pelaku usaha (B2B) atau pelaku usaha dengan konsumen (B2C) yang dilakukan melalui media elektronik.

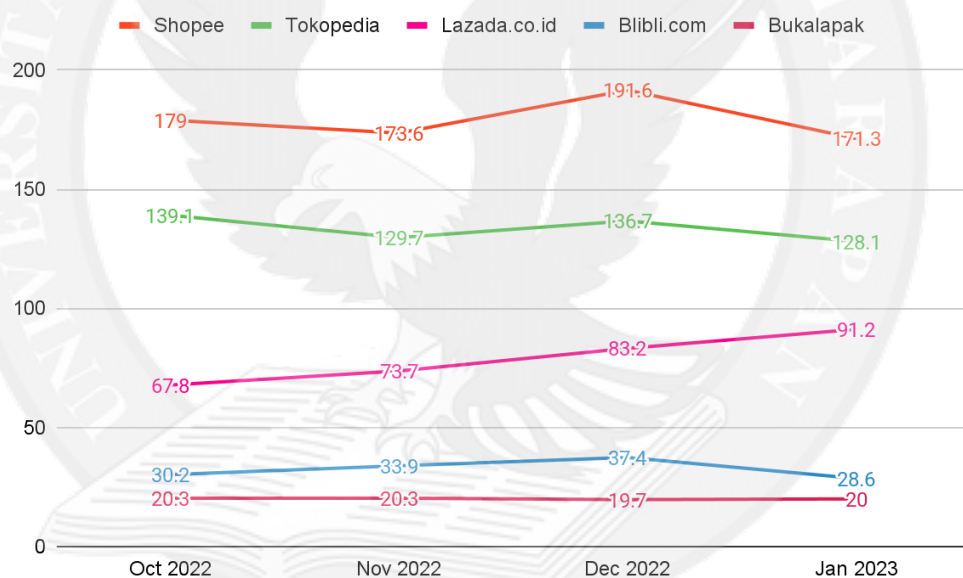
Wadah untuk melakukan transaksi *e-commerce* disebut sebagai *platform*. Menurut Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia *Platform* dan Pedagang (*merchant*) perdagangan melalui Sistem Elektronik (*electronic commerce*) yang berbentuk *User Generated Content*, batasan istilah *platform* adalah sebagai berikut:

“*Platform* adalah wadah berupa aplikasi, situs internet, dan/atau layanan konten lainnya berbasis internet yang digunakan untuk transaksi dan/atau fasilitasi perdagangan melalui sistem elektronik”⁶

⁵ “In general, selling and buying electronically can be either business-to-consumer (B2C) or business-to-business (B2B).” in Efraim Turban, Jon Outland, David King, Jae Kyu Lee, Ting-Peng Liang, & Deborah C. Turban. *Electronic Commerce 2018: A Managerial and Social Networks Perspective, Ninth Edition*. (Switzerland: Springer International Publishing, 2018). Hlm 8.

⁶ Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia *Platform* dan Pedagang (*Merchant*) perdagangan melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk *User Generated Content*. V.A.1. Hlm 5.

Berdasarkan penjelasan tersebut, *marketplace* dapat diartikan sebagai sebuah tempat berupa *platform digital* yang memberikan kemudahan bagi para pembeli dan penjual untuk melakukan transaksi secara elektronik. Tujuannya ialah mencapai terjadinya transaksi ekonomi, terlepas dari lokasi fisik sang pembeli maupun penjual. Berdasarkan data jumlah kunjungan pada Gambar 1.2. yang bersumber dari *similarweb.com*, 5 (lima) *marketplace* di Indonesia yang paling ramai dikunjungi pada akhir tahun 2022 hingga awal tahun 2023 adalah Shopee dari Singapura, Tokopedia, Lazada yang dimiliki Alibaba Group dari Cina, Blibli.com dari Indonesia, dan Bukalapak.



Gambar 1.2. Lima *Marketplace* dengan Jumlah Kunjungan Situs Terbanyak di Indonesia⁷

Transaksi elektronik yang melibatkan berbagai pihak secara *virtual* memerlukan identifikasi identitas para pelaku transaksi. Hal ini menyebabkan

⁷ Similarweb, “Top *Marketplace* Websites in Indonesia“, <https://www.similarweb.com/top-websites/indonesia/e-commerce-and-shopping/marketplace/>, diakses 26 Februari 2023, pukul 01:31 WIB.

informasi data pribadi milik pembeli (konsumen) dan pelaku usaha (penjual) menjadi sebuah komoditas yang ditukarkan. Cakupan yang diambil dari interaksi tersebut meliputi pengumpulan data pribadi, pemrosesan, penyimpanan, pengiriman, dan produksi. Setiap interaksi dapat berjalan dengan lancar ketika diberi akses data pribadi seperti data diri, nomor kontak, alamat, dan lain sebagainya.⁸

Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dalam Pasal 1 Ayat 1 data pribadi didefinisikan sebagai berikut:

“Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.”⁹

Menurut Karo & Prasetyo, data pribadi dapat diartikan sebagai berikut:

“Informasi tunggal ataupun sekumpulan informasi baik yang bersifat rahasia ataupun tidak yang diberikan oleh pemilik data pribadi/konsumen dan dihimpun ke dalam sistem elektronik yang diproses oleh penyelenggara sistem elektronik untuk dipergunakan sesuai dengan tujuan & kegunaannya serta apabila disalahgunakan maka pemilik/konsumen dapat menyelesaikannya melalui media hukum administrasi negara dan/atau media hukum perdata dan/atau media hukum pidana.”¹⁰

Berdasarkan kedua pengertian di atas, data pribadi terdiri dari informasi milik individu yang diproses dan disimpan bersama dengan informasi lainnya dalam suatu sistem elektronik. Pengertian privasi tidak sebatas kebebasan individu

⁸ Sinta Rosadi Dewi dan Dinah Sumayyah, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, (Bandung: Refika Aditama, 2015), Hlm 23.

⁹ Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

¹⁰ Rizky P.P. Karo Karo & Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*, (Bandung: Penerbit Nusa Media, 2020), Hlm 50.

pada sebuah ruang fisik, melainkan juga ruang individu yang turut memiliki kebebasan dalam ruang *digital*. Dalam konteks ini, ruang *digital* yang dimaksud adalah *marketplace*, tempat terjadinya transaksi elektronik yang turut melibatkan penggunaan data pribadi untuk kepentingan ekonomi.

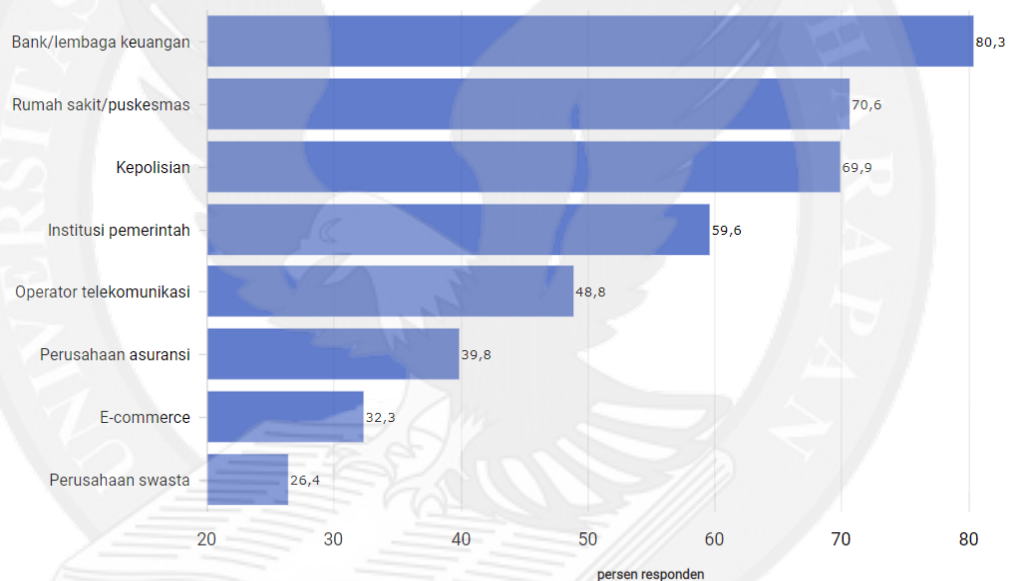
Menurut Riadi, privasi dapat dimengerti sebagai sebuah persetujuan yang bersifat spesifik dan pemberitahuan mengenai prosedur dan sistem regulasi yang dilakukan dalam sebuah manajemen data. Perlindungan data pribadi menyangkut keamanan data (*data security*) dan privasi data (*data privacy*) yang melibatkan dua unsur, yaitu aspek teknologi dan aspek hukum. Privasi data merupakan sebuah kesepakatan dan notifikasi yang diberikan secara prosedural melalui sistem manajemen data yang melindungi hak konsumen dan perusahaan.¹¹

Melalui sistem *digital*, data pribadi menjadi sebuah aset bernilai ekonomis tinggi yang dapat berakibat pada rentannya terjadi kebocoran data pribadi demi keuntungan ekonomis.¹² Data pribadi tidak terbatas pada sebuah informasi yang dimasukkan dalam sistem elektronik, melainkan sebuah sarana bagi perusahaan-perusahaan untuk melakukan perluasan pasar melalui pemetaan karakteristik para konsumen. Secara ekonomis, penggunaan data pribadi dapat dijadikan sebuah strategi bisnis dalam perkembangan teknologi *digital*.

¹¹ Gliddheo Riadi, "Data *Privacy* in the Indonesian Personal Data Protection Legislation", Policy Brief, No. 7 March 2021 (Jakarta: Center for Indonesian Policy Studies (CIPS)), Hlm 2.

¹² Kean Birch, D.T. Cochrane, & Callum Ward, "Data as asset? The measurement, governance, and valuation of *digital* personal data by Big Tech", *Big Data & Society*, Vol. 8, No. 1 May 2021, Hlm 1. <https://doi.org/10.1177/20539517211017308>

Data pribadi sebagai sebuah aset bisnis bisa disalahgunakan. Menurut survei Kementerian Komunikasi dan Informatika bersama Katadata Insight Center (KIC) yang dapat dilihat pada Gambar 1.3., *e-commerce* menempati posisi ke-7 dengan persentase kepercayaan responden sebesar 32,3%. Hal ini menunjukkan bahwa kepercayaan publik terhadap *e-commerce* untuk melindungi data pribadi cukup rendah. Survei tersebut dilakukan selama periode 14-21 Juli 2021 terhadap 11.305 responden yang tersebar di 34 provinsi Indonesia.

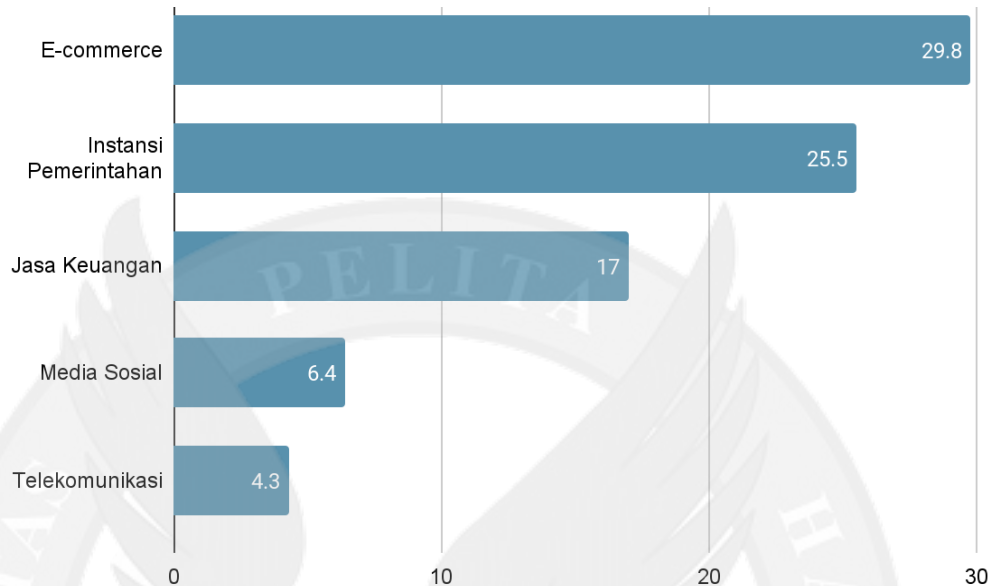


Gambar 1.3. Lembaga yang Dipercaya Responden Mampu Melindungi Data Pribadi Dalam Persentase (2021)¹³

Dalam sebuah laporan *IDX Channel* pada tahun 2022 yang dapat dilihat pada Gambar 1.4., persentase kasus peretasan hingga kebocoran data *e-commerce* yang terjadi dari tahun 2019-2022 ialah sebesar 29,8%. Angka ini

¹³ Katadata Media Network, “Lembaga yang Dipercaya Responden Mampu Melindungi Data Pribadi (2021)”, <https://databoks.katadata.co.id/datapublish/2022/10/16/ini-lembaga-yang-paling-mampu-lindungi-data-pribadi-menurut-warga-ri>, diakses 25 Februari 2023, pukul 15:32 WIB

menunjukkan *e-commerce* sebagai sektor yang mengalami peretasan tertinggi, lebih tinggi daripada instansi pemerintah dan jasa keuangan.



Gambar 1.4. Kejahatan Siber Berupa Peretasan Hingga Data Bocor Dalam Persentase (2019-Januari 2022)¹⁴

Selanjutnya, menurut *dataindonesia.id* dalam bulan Januari sampai Agustus 2022 telah ditemukan kebocoran data sebanyak 13,89 juta.¹⁵ Kasus kebocoran data Tokopedia, Bukalapak, dan RedMart milik Lazada sempat menarik perhatian publik. Di sisi lain, Bukalapak melaporkan kasus peretasan dan kebocoran data atas 13,000,000 (tiga belas juta) akun dalam sistem databasanya.¹⁶ Sedangkan, Tokopedia melaporkan mengalami kebocoran data

¹⁴ IDX Channel, “Deretan Kebocoran Data *E-commerce* dan Sektor Perbankan, Seberapa Bahaya?”, <https://www.idxchannel.com/economics/deretan-kebocoran-data-e-commerce-dan-sektor-perbankan-seberapa-bahaya/all>, diakses 25 Februari 2023, pukul 16:03 WIB

¹⁵ “Berdasarkan sebuah perusahaan asal Belanda, *Surfshark*, ditemukan bahwa Indonesia menempati posisi keempat sebagai negara yang mengalami kebocoran data sebanyak 13,890,000”. DataIndonesia.id, “Peta Kebocoran Data Global Sepanjang 2022, Termasuk Indonesia”, <https://dataindonesia.id/digital/detail/peta-kebocoran-data-global-sepanjang-2022-termasuk-indonesia>, diakses pada 16 Februari 2022, 23:07 WIB.

¹⁶ Giosita Kumalaratri & Yunanto, “Urgency of The Personal Protection Bill on *Privacy Rights* in Indonesia”, *Jurnal Hukum Unissula*, Vol. 37, No. 1 Mei 2020, Hlm 3.

sekitar 91,000,000 (sembilan puluh satu juta) akun pembeli dan 7,000,000 (tujuh juta) akun penjual (*merchant*).

Kebocoran data yang dialami Tokopedia disebabkan oleh seorang peretas internasional dengan alias “*Why So Dank*” pada tanggal 17 April 2020. Peredaran informasi mengenai kasus peretasan ini terjadi melalui sebuah media sosial *Twitter*. Akun *underthebreach* memberikan informasi mengenai *email*, *password*, serta nama pengguna. Menurut pengakuan akun tersebut, peretasan telah membocorkan sekitar 15,000,000 (lima belas juta) data pengguna Tokopedia. Namun, setelah ditelusuri lebih lanjut, data yang berhasil diretas bertambah menjadi 91,000,000 (sembilan puluh satu juta) akun pembeli dan 7,000,000 (tujuh juta) akun penjual (*merchant*). Hal tersebut menunjukkan hampir semua akun dalam *marketplace* Tokopedia telah diretas. Hasil dari peretasan tersebut dijual oleh pelaku sebesar USD 5000 atau sekitar Rp 74,000,000 di *dark web*, yaitu *Raid Forums*.¹⁷

Dalam kasus ini, secara hukum, terdapat suatu prinsip yang terlanggar. Menurut teori *negligence*, disebutkan bahwa “*the failure to exercise the standard of care that reasonably prudent person would have exercised in a similar situation*”¹⁸ atau dalam Bahasa Indonesia “ketidakmampuan untuk menerapkan standar kepedulian yang sejatinya perlu dilakukan oleh seseorang secara cermat dalam situasi yang sama.” Hal ini dapat dilihat dalam kebijakan

¹⁷ Muhammad Fathur, “Tanggung Jawab Tokopedia terhadap Kebocoran Data Pribadi Konsumen”, *National Conferences on Law Studies: Legal Development towards A Digital Society Era* (2020), Hlm 46. ISBN: 978-979-3599-13-7.

¹⁸ Brian A. Gaener, *Black's Law Dictionary*, (St. Paul, MN: Thomson Reuters, 2014), Hlm 1061.

privasi yang tertera dalam *platform* Tokopedia yang memberikan sebuah ruang untuk tidak bertanggungjawab apabila terjadi sebuah peretasan:

“Setiap informasi/data Pengguna yang disampaikan kepada Tokopedia dan/atau yang dikumpulkan oleh Tokopedia dilindungi dengan upaya sebaik mungkin oleh perangkat keamanan teruji, yang digunakan oleh Tokopedia secara elektronik. Meskipun demikian, Tokopedia tidak menjamin kerahasiaan informasi yang Pengguna sampaikan tersebut, dalam kondisi adanya pihak-pihak lain yang mengambil atau mempergunakan informasi Pengguna dengan melawan hukum serta tanpa izin Tokopedia.”¹⁹

Menindaklanjuti kasus kebocoran tersebut, Komunitas Konsumen Indonesia melayangkan gugatan di Pengadilan Negeri Jakarta Pusat kepada Menteri Komunikasi dan Informatika dan PT Tokopedia pada 8 Mei 2020.²⁰ Dalam prosesnya, gugatan tersebut ditolak oleh Pengadilan Negeri, Pengadilan Tinggi, dan Kasasi dengan menimbang Undang-Undang Nomor 30 Tahun 2014 Pasal 87, hal yang demikian adalah menjadi ruang lingkup kewenangan Peradilan Tata Usaha Negara. Oleh karena itu, menurut hakim gugatan seharusnya diajukan kepada Peradilan Tata Usaha Negara bukan peradilan umum.²¹

Selain kasus kebocoran data pada beberapa *marketplace* besar di Indonesia, terdapat juga kebocoran data pada instansi pemerintah. Peretas yang

¹⁹ Emmy Febriani Thalib & Ni Putu Suci Meinarni, “Tinjauan Yuridis Mengenai *Marketplace* Berdasarkan Peraturan Perundang-Undangan di Indonesia”, *Jurnal IUS*, Vol. 7, No. 2 Agustus 2019, Hlm 201.

²⁰ SIPP Pengadilan Negeri Jakarta Pusat, Nomor Perkara Nomor 235/PDT.G/2020/PN.JKT.PST, http://sipp.pn-jakartapusat.go.id/index.php/detil_perkara, diakses 15 September 2023, pukul 19:35 WIB.

²¹ JDIH Kementerian Komunikasi dan Informatika RI, “Nomor Perkara: No. 235/PDT.G/2020/PN.JKT.PST”, <https://jdih.kominfo.go.id/perkara/view/21>, diakses pada 15 September 2023, pukul 19:35 WIB

menggunakan alias *Bjorka* turut mengambil perhatian publik pada September 2022. Lebih dari satu kali, peretas *Bjorka* mengaku menyebarkan informasi pribadi mengenai nomor telepon pribadi dari anggota kementerian, membocorkan 26,700,000 (dua puluh enam juta tujuh ratus ribu) data pelanggan IndiHome, 1,300,000,000 (satu miliar tiga ratus juta) data *sim card*, serta 105,000,000 (seratus lima juta) data pemilih dari Komisi Pemilihan Umum (KPU). Tidak hanya itu, *Bjorka* juga membocorkan 679,180 (enam ratus tujuh puluh sembilan ribu seratus delapan puluh) dokumen kepresidenan yang merupakan surat-surat rahasia dari Badan Intelijen Negara (BIN).²²

Secara umum, diperlukan kesadaran masyarakat terhadap privasi data pribadi. Pada tahun 2017, hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menemukan bahwa 65,98% dari responden menyadari bahwa data pribadi mereka dapat diambil melalui *platform digital*. 61,38% dari responden menjawab bahwa menjaga kerahasiaan data adalah hal yang “penting”.²³ Walau demikian, sampai pada tahun 2022, 13,03% dari responden tersebut mengalami kasus keamanan data.²⁴

Berdasarkan paparan data-data di atas, dapat dilihat bahwa pengguna internet di Indonesia mempunyai pengetahuan tentang pentingnya perlindungan data pribadi. Namun, pengetahuan tersebut belum tentu diikuti dengan tingkat kewaspadaan yang sama untuk melindungi data pribadi secara mandiri. Hal ini

²² Amelia Yesidora, "Menguji Kedigdayaan Tim Darurat Bjorka dan Para Peretas Data", <https://katadata.co.id/rezzaaji/indepth/6324822d175ce/menguji-kedigdayaan-tim-darurat-bjorka-dan-para-peretas-data>, diakses pada 20 Mei 2023, Pukul 11:35 WIB.

²³ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Penetrasi & Perilaku Pengguna Internet Indonesia 2017.

²⁴ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Profil Internet Indonesia 2022.

juga didukung oleh sebuah survei nasional pada tahun 2021 yang diselenggarakan oleh *Katadata Insight Center* yang menyimpulkan persepsi masyarakat atas perlindungan data pribadi masih tergolong “belum cukup baik”.²⁵

Studi menunjukkan sejak tahun 2011 sampai 2017, negara-negara Uni Eropa dan Barat sudah menerapkan hukum perlindungan data pribadi dalam kerangka hukum privasi.²⁶ Demikian juga dengan negara-negara di Asia Timur dan Asia Tenggara seperti Tiongkok, Korea Selatan, dan Singapura.²⁷ Sebaliknya, kerangka hukum di Indonesia masih mencoba untuk menerapkan hukum internasional mengenai perlindungan data pribadi.²⁸ Hukum mengenai privasi dan transaksi elektronik yang berlaku pada tahun 2011-2017 belum memberikan definisi yang eksplisit tentang data pribadi, sehingga rentan untuk disalahgunakan demi kepentingan industri maupun lainnya.²⁹

Pada saat kasus-kasus ini terjadi, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi masih dalam proses perancangan. Undang-Undang yang berlaku saat itu ialah Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan

²⁵ Katadata Insight Center, “Persepsi Masyarakat Atas Pelindungan Data Pribadi: Survei Nasional Tahun 2021”, <https://kic.katadata.co.id/insights/43/persepsi-masyarakat-atas-pelindungan-data-pribadi>, Hlm. 60.

²⁶ Agata Syafira Ramadhani, “Komparasi Pengaturan Perlindungan Data Pribadi di Indonesia dan Uni Eropa”, *Jurnal Hukum Lex Generalis*, Vol. 3, No. 1 Januari 2021, Hlm 79.

²⁷ Diana Setiawati, Hary Abdul Hakim, Fahmi Adam Hasby Yoga, “Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore”, *Indonesian Comparative Law Review*, Vol. 2, No. 2 June 2019, Hlm 104-106. <http://dx.doi.org/10.18196/iclr.2219>.

²⁸ Sinta Dewi Rosadi, “Protecting *Privacy* on Personal Data in *Digital* Economic Era: Legal Framework in Indonesia”, *Brawijaya Law Journal*, Vol. 5, No. 1 April 2018, Hlm 154-156.

²⁹ Sinta Rosadi Dewi, “Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia”, *Jurnal De Jure*, Vol. 15, No. 2 Juni 2015, Hlm 27.

Transaksi Elektronik yang masih belum cukup memadai mengenai pengaturan perlindungan data pribadi secara eksplisit.³⁰

Menurut hukum yang berlaku saat itu, terdapat aparatus-aparatus negara yang berfungsi untuk mencegah terjadinya kebocoran data, khususnya di kalangan pemerintahan.³¹ Kementerian informasi dan komunikasi (kominfo) berfungsi untuk merumuskan, menetapkan, dan melaksanakan peraturan-peraturan mengenai pemeliharaan siber. Hal ini turut dijelaskan dalam Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika Pasal 34 yang berbunyi demikian:

“Setiap unsur di lingkungan Kominfo dalam melaksanakan tugasnya harus menerapkan prinsip koordinasi, integrasi, dan sinkronisasi baik dalam lingkungan Kementerian Komunikasi dan Informatika maupun dalam hubungan antar instansi pemerintah baik pusat maupun daerah. Artinya Kominfo yang memiliki peran sebagai jembatan komunikasi antar lembaga siber, sehingga koordinasi dan kerja sama dalam lingkungan lembaga siber dapat berjalan dengan baik, hal ini akan berdampak besar pada kemampuan solid lembaga tersebut dalam menjaga dan mencegah kebocoran data atau serangan siber lainnya yang berisiko terjadi”.

Terdapat pula Badan Siber dan Sandi Negara (BSSN) di bawah Presiden dan berfungsi untuk melakukan penyusunan, pelaksanaan, dan evaluasi kebijakan terhadap serangan siber. Badan tersebut berkewajiban untuk menjalankan tugas dan fungsi kebijakan-kebijakan keamanan siber yang bersifat teknis dan operasional. Dalam hal ini, BSSN berfungsi untuk

³⁰ Universitas Indonesia: Fakultas Ilmu Administrasi, “UU Perlindungan Data Pribadi dan Tantangan Implementasinya”, <https://fia.ui.ac.id/2022/09/21/>, diakses 11 November 2022, pukul 16:10 WIB.

³¹ Apryan Anggara Pratama & Muhammad Ruhly Kesuma Dinata, “*Hacker* Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data”, *Jurnal Hukum Magnum Opus*, Vol. 6, No. 1 Februari 2023, Hlm 14-26. <https://doi.org/10.30996/jhmo.v6i1.8293>

melakukan pemulihan terhadap kerusakan-kerusakan siber. Lembaga tersebut juga turut bekerja dalam melakukan hubungan kerja sama secara nasional maupun internasional.

Walau demikian, pelaksanaan eksekutif dari badan-badan instansi pemerintahan membutuhkan sebuah kerangka hukum. Sejak tahun 2008, Undang-Undang Informasi dan Transaksi Elektronik menjadi hukum utama untuk pertukaran informasi *digital*. Berikut adalah beberapa pasal yang berhubungan dengan privasi individu dalam bentuk data elektronik menurut Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

1. Pasal 27 Ayat (3)

“Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik.”

2. Pasal 32 Ayat (1)

“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan atau dokumen elektronik milik orang lain atau milik publik.”

3. Pasal 32 Ayat (2)

“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.”

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik belum memberikan definisi mengenai “data pribadi”. Data pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik dimengerti sebagai hak privasi (*privacy rights*) yang dimiliki individu. Identifikasi pihak-pihak yang terlibat dalam penyalahgunaan atau pembocoran data belum dibahas dalam kerangka hukum tersebut. Kebocoran data rentan terjadi ketika data pribadi diserahkan kepada suatu instansi publik, seperti pemerintahan atau organisasi swasta. Dalam hal ini, hak dan kewajiban pihak pengendali data pribadi masih belum dijelaskan secara eksplisit dalam ranah hukum.³²

Pada tanggal 17 Oktober 2022, Presiden Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang sebelumnya telah disahkan oleh DPR pada tanggal 20 September 2022. Setelah kurang lebih tujuh tahun dalam proses penyusunan, Undang-undang baru ini hadir sebagai respon terhadap fenomena teknologi *digital* di masyarakat. Salah satu subjek hukum yang dituju oleh peraturan ini adalah perusahaan-perusahaan penyelenggara *platform marketplace* di Indonesia sebagai pengendali data pribadi. Dengan demikian, undang-undang tersebut berfungsi sebagai payung hukum yang terbaru untuk melengkapi yang belum tercakup dalam Undang-Undang Informasi dan Transaksi Elektronik.

Disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan sebuah definisi hukum sebagai berikut:

³² I Putu Bayu Mahendra & I Dewa Gede Dana Sugama, “Perlindungan Data Pribadi Konsumen Daring Pada Saat Bertransaksi *E-commerce* di Indonesia”, Jurnal Kertha Desa, Vol. 8, No. 12 Januari 2021, Hlm 43. <https://ojs.unud.ac.id/index.php/kerthadesa/article/view/69286>.

1. Pasal 4 Ayat (2)

“Data pribadi yang bersifat spesifik, meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi; dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.”

2. Pasal 4 Ayat (3)

“Data pribadi yang bersifat umum, meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.”

3. Pasal 47

“Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Perlindungan Data Pribadi.”

Undang-undang ini membagi data pribadi menjadi dua, yaitu yang bersifat spesifik dan bersifat umum. Dalam Pasal 47 ditekankan tanggung jawab pemrosesan dan perlindungan data pribadi dijatuhkan kepada pengendali data pribadi atau dalam konteks *marketplace* ialah penyedia *platform*. Bila perusahaan atau lembaga pengendali data pribadi gagal untuk melindungi data pribadi subjek data yang dimilikinya, maka terdapat sanksi sebagai ganjarannya. Sanksi yang diberikan diatur dalam Pasal 46 yang berbunyi sebagai berikut:

1. Pasal 46, Ayat (1)

“Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: a. Subjek Data Pribadi; dan b. Lembaga.”

2. Pasal 46 Ayat (2)

“Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat:

- a. Data Pribadi yang terungkap;
- b. Kapan dan bagaimana Data Pribadi terungkap; dan
- c. Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.”

3. Pasal 46 Ayat (3)

“Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.”

Penjelasan lebih spesifik mengenai pihak-pihak yang terkait dalam manajemen data pribadi telah memberikan kedudukan hukum tentang hak dan kewajiban para pelaku transaksi di *marketplace*. Upaya pemerintah dalam menyusun kerangka hukum mengenai perlindungan data pribadi akan mengubah pola hubungan transaksi elektronik dan manajemen data antara pihak pembeli, pelaku usaha, dan penyelenggara *platform marketplace*. Dari pihak pembeli barang, kesadaran akan penggunaan teknologi, hukum, dan kepercayaan akan *marketplace* menjadi faktor penting dalam pemberian data pribadi. Sebaliknya, dari pihak penyedia *platform*, peraturan pemerintah menjadi sarana untuk menerapkan kebijakan dan mengatur hubungan antara *stakeholders*.³³

Hal ini selaras dengan kajian yang dilakukan oleh Pusat Penelitian Badan Keahlian Sekretariat Jenderal DPR RI pada tahun 2020 yang menyatakan perlindungan data pribadi konsumen dalam era *digital* belum optimal.³⁴ Keadaan belum optimal ini didukung oleh beberapa jurnal hukum terdahulu

³³ Sfenrianto Sfenrianto, Tendi Wijaya & Gunawan Wang, “Assessing the Buyer Trust and Satisfaction Factors in the E-Marketplace”, *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 13, No. 2 May 2018, Hlm 50.

³⁴ Trias Palupi Kurnianingrum, “Urgensi Perlindungan Data Pribadi Konsumen di Era Ekonomi *Digital*”, *Kajian* Vol. 25, No. 3 Tahun 2020, Hlm 197-216.

yang menyimpulkan penyelenggara *platform marketplace* bertanggung jawab terhadap data pribadi,³⁵ namun ketiadaan undang-undang mengenai perlindungan privasi³⁶ menyebabkan masyarakat sulit untuk menuntut tanggung jawab dari penyelenggara *platform marketplace* terkait kebocoran data.³⁷ Menanggapi pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sebuah jurnal hukum yang diterbitkan awal tahun ini menyimpulkan bahwa perlindungan hukum terhadap data konsumen *marketplace* di Indonesia telah diatur dalam undang-undang tersebut.³⁸

Berdasarkan uraian di atas, penulis selaku mahasiswa hukum tertarik untuk menganalisis permasalahan tersebut dan menuangkannya ke dalam karya tulis ilmiah yang berjudul “Pengaturan Hukum Terhadap Pelindungan Data Pribadi Pembeli *Marketplace* Di Indonesia.”

1.2 Rumusan Masalah

Sesuai dengan latar belakang di atas, maka penulis merumuskan beberapa masalah sebagai berikut:

³⁵ Kasmawati, et al. “Legal Protection of *Marketplace* Consumer Personal Data in Indonesia”, *International Journal of Multicultural and Multireligious Understanding (IJMMU)*, Vol. 9, No. 8 August 2022, Hlm. 256-266.

³⁶ R. Ayunda, "Personal Data Protection to *E-commerce* Consumer: What Are the Legal Challenges and Certainties?," *LAW REFORM*, Vol. 18, No. 2 August 2022, Hlm. 144-163. <https://doi.org/10.14710/lr.v18i2.43307>

³⁷ Muhammad Raihan, “Perlindungan Data Diri Konsumen dan Tanggungjawab *Marketplace* Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)”, *Jurnal Inovasi Penelitian*, Vol. 3, No. 10 Maret 2023, Hlm 7847-7856.

³⁸ Zendik Anggriawan, Ratih Kemala & Erry Praditya, “Analisis Perlindungan Hukum terhadap Data Konsumen *Marketplace* di Indonesia Berdasarkan Undang-undang No 27 Tahun 2022”, *Journal Humaniora: Jurnal Hukum dan Ilmu Sosial*, Vol. 01, No. 02 April 2023, Hlm. 36-40.

1. Bagaimana pengaturan hukum terhadap perlindungan data pribadi di Indonesia?
2. Bagaimana implementasi perlindungan hukum terhadap perlindungan data pribadi pembeli di *marketplace*?

1.3 Tujuan Penelitian

Berdasarkan latar belakang masalah dan rumusan masalah yang telah disusun, maka tujuan penelitian ini ialah sebagai berikut:

1. Menelaah proses penyelesaian sengketa hukum perlindungan data pribadi berdasarkan studi kasus kebocoran data Tokopedia tahun 2020.
2. Menganalisis persoalan hukum perlindungan data pribadi di Indonesia menurut tinjauan teori dan prinsip hukum.

1.4 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini berupa manfaat teoritis dan manfaat praktis dengan rincian sebagai berikut:

1.4.1 Manfaat Teoritis

Secara teoritis, penelitian ini diharapkan dapat memberikan pemikiran atau masukan dalam ilmu pengetahuan, khususnya terkait dengan hukum perlindungan data pribadi, hukum bisnis dalam ranah ekonomi dan teknologi *digital*.

1.4.2 Manfaat Praktis

Secara praktis, penelitian ini diharapkan dapat memberikan masukan hukum bagi beberapa pihak, antara lain sebagai berikut:

1. Bagi Pemerintah dan anggota Dewan Perwakilan Rakyat diharapkan penulisan tesis ini dapat memberi masukan atau pedoman dalam pembuatan kebijakan ataupun merancang sebuah peraturan perundang-undangan.
2. Bagi para penyelenggara *platform* diharapkan dapat memberikan masukan dan pedoman dalam mentaati regulasi atau kebijakan di Indonesia dalam membuat kebijakan yang lebih baik dalam mengatur hubungan antara *stakeholders marketplace*.
3. Bagi para pembeli barang di *marketplace* diharapkan penulisan tesis ini dapat memberikan pedoman dalam memahami aturan yang memberikan perlindungan dalam ranah data pribadi.

1.5 Sistematika Penulisan

Sistematika penulisan tesis ini terdiri dari lima bab yang meliputi keseluruhan penulisan dengan rincian sebagai berikut:

Bab I : Pendahuluan

Bab I berisikan pendahuluan yang membahas tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan tesis.

Bab II : Tinjauan Pustaka

Bab II berisikan tinjauan pustaka berisikan tinjauan pustaka yang disusun berdasarkan studi kepustakaan, literatur, kamus,

dan jurnal penulisan hukum khususnya mengenai tema penulisan tesis ini.

Bab III : Metodologi Penelitian

Bab III berisikan metodologi penelitian yang meliputi jenis penelitian, jenis data, cara perolehan data, jenis pendekatan, dan analisis data.

Bab IV : Hasil Penelitian dan Analisis

Bab IV berisikan hasil penelitian dan analisis kedua rumusan masalah sesuai dengan tujuan penelitian dalam tesis ini.

Bab V : Kesimpulan dan Saran

Bab V berisikan kesimpulan yang disertai dengan saran bagi pengampu kebijakan dan *stakeholders* yang terlibat dalam *marketplace*, serta memberikan rekomendasi bagi studi akademis berikutnya, khususnya yang berhubungan dengan data pribadi dan *marketplace*.