BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Teknologi selama 2 dekade terakhir mengalami perkembangan yang sangat pesat. Teknologi membuat segala sesuatu menjadi seperti tanpa hambatan (*seamless*), tanpa batasan ruang maupun waktu. Salah satu bentuk aktivitas manusia yang sangat dipermudah yaitu dalam melakukan transaksi jual beli. Apabila dahulu manusia melakukan transaksi, baik sebagai pelaku usaha maupun sebagai konsumen, harus melakukan pertemuan fisik atau tatap muka, maka pada era digital seperti saat ini, manusia hanya perlu menggunakan perangkatnya yang terhubung dengan jaringan Internet untuk melakukan transaksi melalui platform atau sistem elektronik. Transaksi secara elektronik semacam itu dikenal juga dengan istilah perdagangan melalui sistem elektronik atau *e-commerce*[1].

Dengan terjadinya perkembangan teknologi yang begitu pesat, tidak dapat dipungkiri bahwa akan memengaruhi norma hukum yang berkembang, baik norma privat atau publik[2]. Beberapa masalah juga mungkin akan muncul, termasuk dalam hal perlindungan data pribadi dan masalah pada sektor *e-commerce*[3]. Terlepas dari sekian banyaknya manfaat, keuntungan, kenyamanan dan kemudahan yang didapatkan oleh konsumen *e-commerce*, sebenarnya melakukan transaksi jual beli secara daring juga memaparkan konsumen pada berbagai risiko, salah satunya yaitu

[1] Menurut Pasal 1 angka (2) PP 71/2019, "*Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya*."
[2] Supancana, I.B.R. (2020). *Cyber Ethics* dan *Cyber Law:* Kontribusinya bagi Dunia Bisnis. Edisi 1. Jakarta: Universitas Katolik Indonesia Atma Jaya, hlm. 23
[3] Ibid.

risiko keamanan konsumen, terutama data pribadi dari konsumen sebagai subjek data. Empat risiko utama terkait keamanan siber adalah keamanan transaksional, privasi, keamanan sistem *e-commerce* dan kejahatan dunia maya[4]. Sering kali, pada saat konsumen mendaftar ke platform belanja daring, konsumen diminta untuk memberikan berbagai data pribadi oleh penyelenggara sistem elektronik atau platform belanja tersebut, termasuk, namun tidak terbatas pada, nama, nomor telepon, alamat, alamat surel, dan kata sandi. Namun, sayangnya, data pribadi konsumen sering kali tidak dilindungi dengan baik dan menyeluruh oleh penyelenggara transaksi elektronik dan/atau pelaku usaha yang dalam hal ini bertindak sebagai pengendali dan/atau prosesor data pribadi. Apabila sistem elektronik yang digunakan atau dikelola tidak diberi tingkat perlindungan yang memadai, maka hal tersebut akan sangat mempermudah peretas (*hacker*) untuk membobol sistem tersebut. Keberhasilan pembobolan sistem oleh peretas akan sangat membahayakan keamanan data pribadi dan sensitif dari para konsumen yang tersimpan, terlebih lagi jika data tersebut tidak terenkripsi. Salah satu kejahatan teknologi yang sangat mungkin terjadi adalah pelanggaran data dan pencurian identitas[5]. Penulis berpendapat bahwa pelanggaran data adalah salah satu kejahatan di dunia siber yang paling mengancam. Peretasan dan pelanggaran data sendiri masih sangat susah dilacak sehingga tindak lanjut terhadap pelaku juga akan sangat sulit diterapkan. Dari sisi pengguna atau konsumen sebagai subjek data, langkah-langkah preventif seperti mengganti kata sandi (*password*) secara berkala dan tidak memberitahukan kode *one-time password* (OTP) kepada siapa pun harus dipahami

[4] Nafi'ah, R. (2020). Pelanggaran Data dan Pencurian Identitas pada *E-Commerce*. Cybersecurity dan Forensik Digital. Vol. 3, No.1, hlm. 8
[5] Ibid, hlm. 9.

dan diterapkan oleh pengguna teknologi, pengguna sistem elektronik, terutama konsumen yang berbelanja di platform *e-commerce*.

Di Indonesia sendiri, terjadi banyak sekali kasus kebocoran data dan kasus paling banyak terjadi dalam sektor belanja daring[6]. Salah satu sumber menyatakan bahwa dari 277 kasus kebocoran data dari bulan Januari sampai Juni 2020, 54 kasus di antaranya adalah kasus pencurian data belanja *online*. Hal ini tentunya sangat meresahkan bagi konsumen yang melakukan transaksi elektronik. Padahal, pelaku usaha harus menyimpan data pribadi konsumen sesuai dengan standar perlindungan data pribadi atau kelaziman praktik bisnis[7]. Terlepas dari sudah adanya pengaturan lebih lanjut mengenai kelaikan dan standar keamanan sistem elektronik serta perlindungan data pribadi konsumen dalam rangka perdagangan secara elektronik sebagaimana diatur dalam PP No. 71 Tahun 2019[8] dan PP No. 80 Tahun 2019[9] sebagai turunan dari UU ITE[10], ternyata faktanya menunjukkan bahwa bahkan platform-platform *e-commerce* terbesar di Indonesia pun masih sangat rentan terhadap pembobolan oleh peretas. Hal ini tentu akan memiliki dampak terhadap keengganan konsumen untuk menggunakan platform *e-commerce* karena konsumen dihantui dengan rasa ketidakamanan dan ketidaknyamanan untuk menggunakan platform elektronik dalam rangka melakukan transaksi elektronik.

Pada bulan Maret 2020 lalu, telah terjadi satu kasus pelanggaran data yang sangat marak diperbincangkan yang dialami oleh salah satu platform belanja daring

[6] https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan
[7] Pasal 59, Peraturan Pemerintah Republik Indonesia No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
[8] PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
[9] PP No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik
[10] Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

terbesar di Indonesia, yaitu Tokopedia. Menurut CNBC Indonesia[11], terdapat sebanyak 91 juta data pengguna Tokopedia yang diretas dan dijual di *dark web* seharga US$5.000. Tokopedia memberi pernyataan bahwa memang benar adanya upaya peretasan yang dilakukan terhadap sistem mereka. Dalam peretasan tersebut, data yang berhasil diretas adalah data berupa nama pengguna, *e-mail*, *hash password*, tanggal lahir, kode aktivasi *e-mail*, kode reset *password*, detail lokasi, ID messenger, hobi, pendidikan, waktu pembuatan akun dan bahkan waktu terakhir *login*[12]. Menurut salah satu advokat bernama David Tobing, pelanggaran data yang terjadi dalam *e-commerce* salah satunya disebabkan karena data yang diminta platform sudah berlebihan dan sebenarnya tidak relevan dengan tujuan untuk berbelanja di *marketplace*[13]. Menurut penulis, sebagian dari data yang diminta di platform *e-commerce* sebenarnya bersifat *redundant* dan kerap kali, data yang diminta oleh penyelenggara sistem elektronik dilakukan pemrosesan oleh pengendali dan/atau prosesor data pribadi untuk keperluan yang tidak sesuai dengan tujuan awal dimintanya data pribadi dari subjek data. Data yang *redundant* seperti ini akan sangat membahayakan keamanan, keselamatan hingga reputasi subjek data jika data tersebut jatuh ke tangan yang salah karena *database* data pribadi sangat berkemungkinan besar untuk disalahgunakan dan kemudian merugikan subjek data, baik secara materiil maupun immateriil.

Konsumen melakukan transaksi secara elektronik melalui platform belanja elektronik adalah karena pembeli bisa mengakses informasi mengenai harga dan

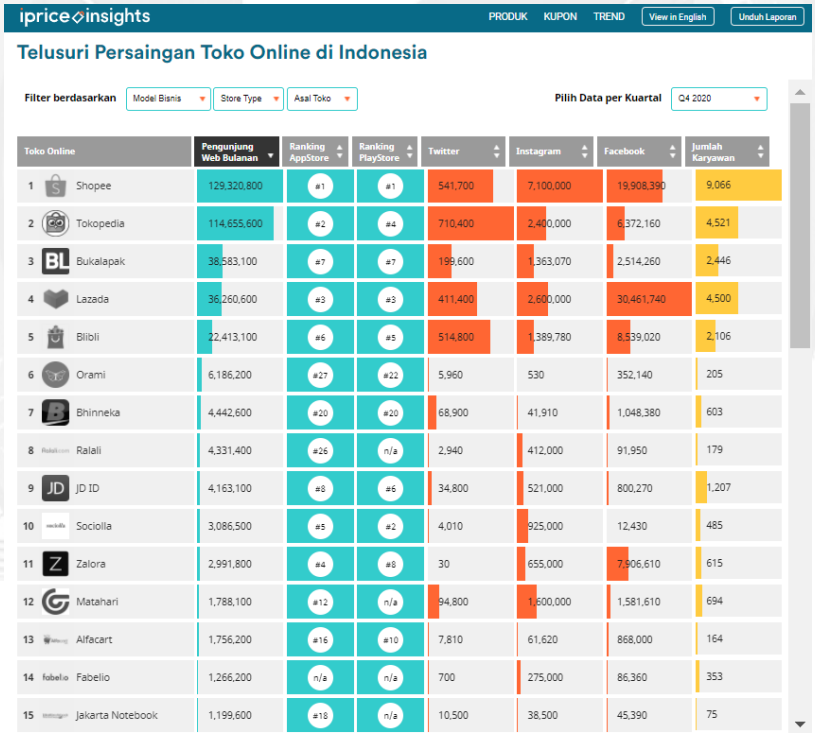
---

[11] https://www.cnbcindonesia.com/tech/20200704112811-37-170183/kacau-banget-kok-bisa-sih-data-tokopedia-bocor

[12] https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all

[13] https://www.hukumonline.com/berita/baca/lt5e57416828b4b/urgensi-perlindungan-data-pribadi-konsumen-di-sektor-e-commerce?page=all

perbedaan harga antara satu penjual dengan penjual lain serta mendapatkan informasi mengenai produk-produk pengganti yang ada di *marketplace*[14]. Selain itu, keuntungan lain dari *e-commerce* adalah konsumen bisa melakukan transaksi tanpa batasan waktu (24 jam sehari) dan tidak perlu berinteraksi secara fisik dengan penjual dan transaksi bisa dilakukan di mana saja[15] dengan catatan adanya jaringan Internet. Dengan kata lain, konsumen bisa mendapatkan kenyamanan dari segi waktu, tempat, kontak dan interaksi, serta perbandingan produk di pasar dengan berbelanja secara daring (*online*) melalui platform-platform *e-commerce*. Beberapa platform *e-commerce* terbesar di Indonesia saat ini meliputi Shopee, Tokopedia, Bukalapak, Lazada, Blibli.



	Toko Online	Pengunjung Web Bulanan	Ranking AppStore	Ranking PlayStore	Twitter	Instagram	Facebook	Jumlah Karyawan
1	Shopee	129,320,800	#1	#1	541,700	7,100,000	19,908,390	9,066
2	Tokopedia	114,655,600	#2	#4	710,400	2,400,000	6,372,160	4,521
3	Bukalapak	38,583,100	#7	#7	199,600	1,363,070	2,514,260	2,446
4	Lazada	36,260,600	#3	#3	411,400	2,600,000	30,461,740	4,500
5	Blibli	22,413,100	#6	#5	514,800	1,389,780	8,539,020	2,106
6	Orami	6,186,200	#27	#22	5,960	530	352,140	205
7	Bhinneka	4,442,600	#20	#20	68,900	41,910	1,048,380	603
8	Ralali	4,331,400	#26	n/a	2,940	412,000	91,950	179
9	JD ID	4,163,100	#8	#6	34,800	521,000	800,270	1,207
10	Sociolla	3,086,500	#5	#2	4,010	925,000	12,430	485
11	Zalora	2,991,800	#4	#8	30	655,000	7,906,610	615
12	Matahari	1,788,100	#12	n/a	94,800	1,600,000	1,581,610	694
13	Alfacart	1,756,200	#16	#10	7,810	61,620	868,000	164
14	Fabelio	1,266,200	n/a	n/a	700	275,000	86,360	353
15	Jakarta Notebook	1,199,600	#18	n/a	10,500	38,500	45,390	75

Gambar 1. Platform *e-commerce* terbesar yang ada di Indonesia[16]

[14] Khan, A.G. (2016). *Electronic Commerce: A Study on Benefits and Challenges in an Emerging Economy*. Global Journal of Management and Business Research: Economics and Commerce. Vol 16, Ver 1.0, hlm. 19.
[15] Ibid, hlm. 20-21
[16] Sumber dari https://iprice.co.id/insights/mapofecommerce/

Pada kuartal ke-4 tahun 2020, terlihat bahwa Shopee menduduki peringkat pertama dilihat dari jumlah pengunjung per bulan sebanyak 129.320.800 pengunjung dan diikuti dengan Tokopedia di peringkat kedua dengan jumlah pengunjung sebanyak 114.655.600 pengunjung per bulan. Dari sekian banyaknya pengunjung, artinya terdapat data pribadi dalam jumlah yang sangat banyak yang disimpan oleh platform. Konsumen yang melakukan transaksi daring akan sangat rentan terhadap aktivitas yang bersifat menipu. Dengan banyaknya jumlah data pribadi penggunanya, jika tidak dilindungi dengan baik, data akan terpapar tersebut dan sangat berpotensi diperjualbelikan dan disalahgunakan oleh oknum-oknum yang berkepentingan dan mempunyai niat untuk melakukan kejahatan.

Perlu dipahami bahwa untuk sepenuhnya melindungi data pribadi dari penyalahgunaan adalah hal yang mustahil. Salah satu sarana bagi oknum untuk melakukan penyalahgunaan data adalah melalui pelanggaran data. Pelanggaran data (*data breach*) dapat menyebabkan berbagai kerugian, mulai dari kerugian fisik, materiil, bahkan non-materiil terhadap pihak yang menjadi korban. Bahkan beberapa kerugian dapat dilakukan dalam jangka panjang dan berdampak pada kesehatan mental korban. Beberapa bentuk kerugian tersebut seperti pencurian data, penipuan, kerugian finansial, perusakan reputasi, hilangnya kerahasiaan data pribadinya, hingga kerugian ekonomi atau sosial[17]. Pelanggaran dan penyalahgunaan data pribadi akan bisa menyebabkan pihak-pihak yang bersangkutan mendapatkan ancaman baik secara fisik atau batin dengan mempertaruhkan kerahasiaan data pribadinya. Banyaknya informasi sensitif yang

[17] Bisogni, F & Asghari, H. (2020). *More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws*. Journal of Information Policy. Vol. 10, hlm. 50.

berada dalam penguasaan oknum yang mempunyai kepentingan lain dapat berujung pada tindak kejahatan lainnya seperti *phising* yang dapat mengarah pada kejahatan lain, yaitu penipuan dan/atau pemerasan.

Sesungguhnya, pelanggaran data yang kerap terjadi di Indonesia terutama di sektor *e-commerce* merupakan suatu ancaman siber yang bersifat nasional. Kasus-kasus kebocoran data, pelanggaran data, hingga penyalahgunaan data pribadi sesungguhnya sangat merugikan hak konsumen sebagai subjek data. Jika data pribadi konsumen di dunia maya terpapar risiko keamanan begitu saja dan mereka tidak lagi merasa nyaman terutama untuk menggunakan platform *e-commerce*, maka dapat dibayangkan bagaimana ekonomi nasional dan ekonomi digital akan terbentur akibat dampak yang akan muncul.

Keamanan dalam hal *e-commerce* dapat terbagi menjadi beberapa hal yaitu autentisitas, otorisasi, integritas, ketiadaan penyangkalan, kerahasiaan, ketersediaan, privasi[18]. Privasi dapat diartikan bahwa informasi dan data pribadi dari pihak yang bersangkutan tidak diungkapkan kepada publik atau disebarluaskan kepada oknum-oknum lain. Namun, privasi ini sangat berkemungkinan dilanggar oleh pihak-pihak yang mempunyai kepentingan lain, salah satunya dengan melakukan peretasan dan pencurian hingga penyalahgunaan data pribadi.

Saat ini, regulasi terkait perdagangan elektronik diatur dalam Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Pemerintah Republik Indonesia No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Meskipun adanya regulasi-regulasi tersebut, pada kenyataannya, kasus-kasus pelanggaran data

[18] Ibid, hlm. 392.

pribadi yang terjadi menunjukkan bahwa keamanan sistem platform *e-commerce* masih belum memadai yang menunjukkan bahwa tujuan implementasi dan penegakan dari regulasi-regulasi tersebut sesungguhnya belum tercapai. Di samping itu, tidak adanya suatu hukum yang komprehensif tentang perlindungan data pribadi menyebabkan tidak optimalnya penegakan kasus-kasus pelanggaran dan kebocoran data dari sektor *e-commerce*, terutama dalam konteks pertanggungjawaban dari sisi penyelenggara sistem elektronik sebagai pengendali dan/atau prosesor data pribadi serta pengenaan sanksi terhadap pelaku pelanggaran data. Jika hal ini terus terjadi, maka konsumen dalam sektor *e-commerce* akan merasa enggan untuk melakukan transaksi daring dengan menggunakan platform *e-commerce*. Dalam jangka waktu lama, hal ini akan berdampak pada ekonomi dan pendapatan nasional dari sektor digital.

Pengaturan tentang perlindungan data pribadi sendiri sebenarnya sudah ada di Indonesia sebagaimana diuraikan di atas. Namun, perlu menjadi perhatian bahwa pengaturan tersebut masih tersebar di berbagai peraturan yang mengatur masing-masing industri. Beberapa peraturan yang dimaksud tersebut adalah seperti peraturan perlindungan data pribadi untuk industri telekomunikasi dan informatika yang diatur dalam Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi dengan adanya ketentuan larangan melakukan penyadapan[19], dan dalam Undang-Undang No. 11 Tahun 2008 *jo.* Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, di mana dalam UU tersebut, terdapat pasal yang mengatur tentang permintaan izin dari pemilik data jika akan dilakukan pemindahtanganan data. Beberapa pengaturan tentang perlindungan data pribadi

[19] Djafar, W. (2019). *Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan*, hlm. 7

juga diatur dalam peraturan di industri kependudukan dan kearsipan dalam Undang-Undang No. 23 Tahun 2006[20] dan Perpres No. 67 Tahun 2011[21], industri sektor keuangan dan perbankan hingga perpajakan sebagaimana diatur dalam Undang-Undang No. 10 Tahun 1998[22] dan Surat Edaran OJK Nomor 14/SEOJK.07/2014[23], Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik dan beberapa peraturan lain di industri perdagangan, perindustrian, hingga kesehatan. Begitu banyaknya peraturan tentang perlindungan data pribadi yang tersebar di berbagai perundang-undangan untuk industri-industri yang relevan menunjukkan belum adanya standarisasi untuk ruang lingkup pengaturan perlindungan data pribadi, misalnya dari segi jenis data yang dikumpulkan, jenis data apa saja yang tergolong data pribadi, ruang lingkup kewajiban dan tanggung jawab pengendali dan/atau prosesor data, tujuan yang mendasari pemrosesan data pribadi, hak-hak subjek data, serta otoritas perlindungan data pribadi yang tersentralisasi dan terstandarisasi.

Kewajiban dan tanggung jawab penyelenggara sistem elektronik dalam hal perlindungan data pribadi pengguna sistem elektronik juga masih sangat dipertanyakan. Menurut Ketua Badan Perlindungan Konsumen Nasional (BPKN), Ardiansyah Parman, konsumen platform transaksi elektronik sering kali tidak mendapatkan ganti rugi atau jaminan perlindungan yang memadai dari penyelenggara sistem elektronik. Ketua BPKN tersebut menceritakan sebuah kasus

[20] Dalam UU No. 23 Tahun 2006 tentang Administrasi Kependudukan, terdapat ketentuan mengenai kewajiban negara untuk melindungi data pribadi penduduknya
[21] Dalam Perpres No. 67 Tahun 2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, terdapat ketentuan mengenai kewajiban pengumpul data pribadi untuk melindungi kerahasiaan data dan informasi penduduk
[22] Di dalam UU No. 10 Taun 1998 adalah UU Perbankan, diatur mengenai prinsip kerahasiaan bank
[23] SEOJK No. 14/SEOJK/07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Data Pribadi Konsumen

yang pernah terjadi di mana terdapat akun konsumen yang berhasil diambil alih dan kemudian dibajak oleh penjual dengan berbagai upaya untuk *login* dan upaya-upaya lain. Meskipun konsumen sudah melapor kepada pihak penyelenggara platform, namun penyelenggara platform hanya melakukan upaya berupa pemulihan akun dan tidak memberikan ganti rugi apa pun atas kerugian yang diderita oleh konsumen yang menjadi korban *phishing* tersebut. Dari hal tersebut, penulis menyimpulkan bahwa harus diperjelas dan dipertegas sebenarnya apa saja kewajiban dan tanggung jawab penyelenggara platform atau sistem elektronik sebagai pihak pengendali dan/atau prosesor data dalam hal perlindungan data pribadi konsumennya. Hal ini harus diatur dalam satu payung hukum yang komprehensif dan benar-benar mendefinisikan kewajiban dan tanggung jawab pengendali dan/atau prosesor data secara jelas dan tegas agar hak-hak subjek data juga tidak dilanggar begitu saja tanpa mendapatkan kompensasi atau ganti rugi apa pun. Selain itu, penulis juga menemukan bahwa bentuk pertanggungjawaban dari pihak penyelenggara sistem elektronik juga perlu dipertanyakan dan diperjelas dalam hal terjadinya kebocoran data pribadi karena sebagaimana telah diuraikan di atas, implementasi PP No. 71 Tahun 2019, Undang-Undang No. 11 Tahun 2008 *jo.* Undang-Undang No. 19 Tahun 2016, Permenkominfo No. 20 Tahun 2016 serta peraturan-peraturan lain yang berhubungan dengan perlindungan data pribadi dalam hal penyelenggaraan sistem elektronik ternyata belum optimal atau bahkan ketentuan yang diatur di dalam peraturan-peraturan tersebut belum memadai dan dapat diidentifikasi banyak sekali celah sehingga perlu diteliti dan ditelaah apakah diperlukan suatu undang-undang dengan hierarki yang lebih tinggi dan mengatur khusus tentang perlindungan data pribadi demi menjamin hak-hak subjek data.

Setelah melihat dari sisi penyelenggara sistem elektronik sebagai pihak pengendali dan/atau prosesor data pribadi, penulis juga menemukan bahwa dalam PP No. 71 Tahun 2019, Undang-Undang No. 11 Tahun 2008 *jo.* Undang-Undang No. 19 Tahun 2016, Permenkominfo No. 20 Tahun 2016 serta peraturan-peraturan lain yang sudah ada terkait dengan perlindungan data pribadi dalam hal penyelenggaraan sistem elektronik belum diatur secara tegas apa saja sebenarnya hak-hak subjek data sehingga banyak konsumen atau masyarakat pengguna sistem elektronik tidak mengetahui sebenarnya apa saja hak-hak yang mereka miliki sebagai subjek data yang dikumpulkan datanya oleh pihak penyelenggara sistem elektronik. Hal ini tentunya akan sangat merugikan konsumen atau subjek data jika data mereka yang sebenarnya merupakan data pribadi yang tidak seharusnya diketahui publik diminta atau dikumpulkan begitu saja oleh pengendali data, terlebih lagi jika data pribadi tersebut akhirnya jatuh ke tangan peretas atau pihak yang mempunyai niat jahat.

Oleh karena itu, penulis ingin meneliti bagaimana sebenarnya pengaturan tentang perlindungan data pribadi khususnya terkait kewajiban dan tanggung jawab penyelenggara sistem elektronik serta bentuk pertanggungjawaban penyelenggara sistem elektronik dalam hal terjadinya kebocoran dan/atau penyalahgunaan data pribadi pengguna platform serta hak-hak apa saja yang dimiliki oleh konsumen atau pengguna platform sebagai subjek data (*rights of data subject*) dengan cara membandingkan antara peraturan perundang-undangan internasional tentang perlindungan data pribadi, dengan hukum positif yang ada di Indonesia terkait perlindungan data pribadi khususnya dalam penyelenggaraan sistem elektronik

serta rancangan undang-undang perlindungan data pribadi yang kini tengah digodok pembahasannya di DPR.

Penulis menemukan dan membaca beberapa tulisan yang menarik yang membahas tentang perlindungan data pribadi. Salah satu tulisan yang menarik menurut penulis adalah tulisan Haristya S, et al. (2020) yang berjudul "*Studi Pendahuluan: Perbandingan Rancangan Undang-Undang Perlindungan Data Pribadi dengan Konvensi Eropa 109+ dan GDPR*". Dalam tulisan ini, diidentifikasi adanya dua kekurangan yang cukup signifikan yang dapat menjadi penghambat dalam penegakan UU PDP setelah disahkan, yaitu: (1) Pengaturan dalam RUU PDP masih banyak yang tidak terperinci, khususnya terkait perlindungan data, hak subjek data, kewajiban pengendali dan prosesor data, serta transfer data internasional; dan (2) Belum ada ketentuan jelas tentang otoritas perlindungan data dalam RUU PDP. Selain itu, penulis juga menemukan suatu tulisan yang membahas tentang pengaturan perlindungan data pribadi dengan metode penelitian komparasi dengan pengaturan di beberapa negara lain yaitu dalam tulisan Tsamara, N (2021) yang berjudul "*Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara*". Dalam tulisan tersebut dilakukan perbandingan antara pengaturan perlindungan data pribadi di Uni Eropa (EU GDPR), Inggris, Amerika, Hong Kong, Malaysia, Singapura, Korea Selatan, Jepang, dan Indonesia. Dalam tulisan tersebut, disimpulkan bahwa ada beberapa peraturan sektoral yang mengatur perlindungan data pribadi namun masih tidak harmonis dan bahwa pemerintah Indonesia harus membentuk suatu lembaga seperti *Data Protection Agency* di Eropa untuk melaksanakan fungsi kontrol dalam hubungan hukum antara pemilik data dan pengendali data.

Dari kedua tulisan tersebut, maka dapat dilihat bahwa tulisan-tulisan tersebut membahas tentang perlindungan data pribadi secara umum. Maka dari itu, untuk memberikan nilai kebaruan dalam tulisan ini, penulis bermaksud untuk menyelami lebih dalam serta mengembangkan dan melakukan analisis komparatif secara lebih spesifik dengan melihat dari aspek kewajiban dan tanggung jawab pengendali data dan prosesor data, terutama dalam sektor penyelenggaraan sistem elektronik. Penulis hendak meneliti secara lebih khusus tentang kecukupan pengaturan hukum yang ada di Indonesia yang mengatur tentang *e-commerce* dari aspek kewajiban dan tanggung jawab penyelenggara sistem elektronik dalam perannya sebagai pengendali dan/atau prosesor data pribadi serta bagaimana implementasi dan pelaksanaannya di Indonesia dan bagaimana hal tersebut memengaruhi urgensi dari pengesahan RUU PDP.

1.2. Rumusan Pokok Masalah

Dari uraian latar belakang masalah di atas, maka penulis telah merumuskan rumusan pokok masalah yang akan dijawab melalui penelitian dalam tulisan ini, sebagai berikut:

1. Bagaimana pengaturan tentang kewajiban dan tanggung jawab penyelenggara sistem elektronik sebagai pengendali dan/atau prosesor data pribadi dalam penyelenggaraan sistem elektronik?
2. Bagaimana implementasi dan pelaksanaan kewajiban dan tanggung jawab penyelenggara sistem elektronik sebagai pengendali dan/atau prosesor data pribadi berdasarkan kerangka pengaturan yang berlaku di Indonesia?

1.3. Tujuan Penelitian

1. Untuk mengetahui bagaimana pengaturan tentang kewajiban dan tanggung jawab penyelenggara sistem elektronik dalam kapasitasnya sebagai pengendali dan/atau prosesor data pribadi dalam penyelenggaraan sistem elektroniknya dengan melakukan analisis komparatif pengaturan internasional dengan hukum di Indonesia;
2. Untuk mengetahui bagaimana pengaturan tentang hak-hak subjek data dalam penyelenggaraan sistem elektronik oleh penyelenggara sistem elektronik dengan melakukan analisis komparatif pengaturan internasional dengan hukum di Indonesia;

1.4. Manfaat Penelitian

1.4.1 Manfaat Teoritis

Secara teoritis, hasil penelitian yang dilakukan diharapkan dapat menjadi acuan dan referensi dalam mengetahui bagaimana sebenarnya pengaturan tentang perlindungan data pribadi di Indonesia, khususnya terkait kewajiban dan tanggung jawab penyelenggara sistem elektronik dalam kapasitasnya sebagai pengendali dan/atau prosesor data pribadi dalam penyelenggaraan sistem elektroniknya serta pengaturan hak-hak subjek data.

1.4.2 Manfaat Praktis

Secara praktis, hasil penelitian yang dilakukan diharapkan dapat memberi gambaran bagi aparat penegak dan pelaku usaha serta berbagai pemangku kepentingan dan masyarakat tentang bagaimana mereka dapat memberlakukan hak-hak subjek data yang sebenarnya mereka miliki dan memberikan gambaran tentang betapa urgennya pengesahan Rancangan Undang-Undang Perlindungan

Data Pribadi. Penelitian ini juga diharapkan dapat membantu peneliti lain dalam hal referensi dan penyajian informasi jika akan dilakukan penelitian terkait topik perlindungan data pribadi ke depannya.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan adalah bab demi bab, yang akan diuraikan secara singkat sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini, dijelaskan secara garis besar tentang latar belakang dan alasan yang mendasari perlunya dilakukan penelitian ini, yang terdiri dari: Latar Belakang, Rumusan Pokok Masalah, Tujuan Penelitian, Manfaat Penelitian (Manfaat Teoritis dan Manfaat Praktis), dan Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Dalam bab ini, dipaparkan tentang tinjauan umum beberapa kerangka pengaturan internasional dan peraturan perundang-undangan Indonesia yang akan digunakan sebagai bahan analisis serta teori yang digunakan sebagai pisau analisis penelitian ini, yang secara umum terdiri dari Landasan Teori dan Landasan Konseptual.

BAB III. METODE PENELITIAN

Pada bab ini, dijelaskan tentang Pengertian Metode Penelitian, Jenis Penelitian, Sumber dan Sifat Data Penelitian, dan Pendekatan Penelitian.

BAB IV. PEMBAHASAN DAN ANALISIS

Pada bab ini, akan diuraikan secara terperinci tentang jawaban atas rumusan pokok masalah yang dirumuskan pada Bab I dengan melakukan analisis komparatif

pengaturan internasional (*EU GDPR*, *OECD Privacy Guidelines*, dan praktik-praktik di negara Asia), hukum positif Indonesia tentang perlindungan data pribadi, serta dibandingkan juga dengan RUU PDP Indonesia.

BAB V. KESIMPULAN DAN SARAN

Pada bab ini, dimuat kesimpulan dari hal-hal yang telah dijabarkan pada bab-bab sebelumnya dan saran yang dapat diberikan atas kesimpulan dari hal-hal tersebut sebagai penyempurnaan dan peningkatan terhadap isu pokok dari penelitian ini.