

## PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA

*(Legal Protection of Consumer Personal Data in E-Commerce According To Laws  
dan Regulations in Indonesia)*

**Erna Priliyasi**

Badan Pembinaan Hukum Nasional  
Jl. Mayjend Sutoyo 10, Cililitan, Jakarta Timur  
Email: prisqilla@gmail.com

### Abstrak

Transaksi *e-commerce* memberikan banyak keuntungan bagi konsumen dan penjual. Bagi konsumen, *e-commerce* memberikan kemudahan dalam berbelanja tanpa harus datang langsung ke toko fisik. Mereka dapat membandingkan harga dan produk dari berbagai penjual, menghemat waktu dan biaya transportasi. Bagi penjual, *e-commerce* memungkinkan mereka untuk menjangkau pangsa pasar yang lebih luas, meningkatkan visibilitas produk, dan mengoptimalkan proses penjualan dan distribusi. Namun, dalam transaksi *e-commerce*, sering terjadi kebocoran data pribadi konsumen. Kebocoran data pribadi konsumen dalam transaksi *e-commerce* merupakan masalah serius yang dapat mengancam privasi dan keamanan informasi konsumen. Kebocoran data dapat terjadi ketika informasi pribadi seperti nama, alamat, nomor telepon, alamat email, nomor kartu kredit, dan data sensitif lainnya yang seharusnya dijaga kerahasiaannya jatuh ke tangan pihak yang tidak berwenang. Tulisan ini bertujuan untuk mengetahui perlindungan data pribadi konsumen dan mengetahui tanggung jawab *marketplace* atas kebocoran data pribadi konsumen. Penulis menggunakan metode pendekatan yang digunakan dalam penelitian ini adalah yuridis normatif, yaitu metode yang meneliti dan mempelajari bahan-bahan hukum primer dan bahan hukum sekunder. Serta deskriptif Analisis, yaitu menggambarkan peraturan perundang-undangan yang berlaku yang dikaitkan dengan teori-teori hukum dalam pelaksanaan praktik pada masalah yang diteliti. Hasil dari penelitian ini menyimpulkan bahwa di Indonesia telah mempunyai aturan yang secara khusus melindungi data pribadi konsumen yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi Konsumen. Jika terjadi kebocoran data pribadi, maka *marketplace* dapat dikenakan sanksi administratif sesuai peraturan perundang-undangan yang berlaku dan konsumen dapat mengajukan gugatan atas dasar kelalaian *marketplace* sesuai Pasal 1366 KUH Perdata.

**Kata kunci:** marketplace, data pribadi, perlindungan konsumen

### Abstract

*E-commerce transactions provide many advantages for consumers and sellers. For consumers, e-commerce provides convenience in shopping without having to come directly to a physical store. They can compare prices and products from different sellers, saving time and transportation costs. For sellers, e-commerce allows them to reach a wider market share, increase product visibility, and optimize sales and distribution processes. However, in e-commerce transactions, consumer personal data leaks often occur. The leakage of consumer personal data in e-commerce transactions is a serious problem that can threaten the privacy and security of consumer information. Data leaks can occur when personal information such as names, addresses, telephone numbers, email addresses, credit card numbers, and other sensitive data that should be kept confidential fall into the hands of unauthorized parties. This paper aims to determine the protection of consumers' data and find out the responsibility of the marketplace for the leakage of consumers' data. The author uses the approach used in this study as normative juridical, namely the method that examines and studies primary legal materials and secondary legal materials. As well as descriptive analysis, which describes the applicable laws and regulations associated with legal theories in implementing practices on the problems studied. The results of this study conclude that Indonesia already has regulations that specifically protect consumers' data, namely Law Number 27 of 2022 concerning the Protection of Consumer Personal Data. If personal data leakage occurs, the marketplace may be subject to administrative sanctions by applicable laws and regulations and consumers may file a lawsuit based on consumer negligence by Article 1366 of the Civil Code.*

**Keywords:** marketplace, personal data, consumer protection

## A. Pendahuluan

*E-commerce*, atau perdagangan elektronik, telah mengalami perkembangan pesat sejak awal mula kemunculannya pada tahun 1990-an. Dengan adopsi teknologi internet dan perkembangan infrastruktur digital, *e-commerce* telah mengubah cara kita berbelanja dan berbisnis secara mendasar.

*E-commerce* memiliki akar sejarahnya pada tahun 1960-an ketika organisasi bisnis mulai menggunakan *Electronic Data Interchange* (EDI) untuk bertukar dokumen bisnis secara elektronik. Namun, *e-commerce* dalam bentuknya yang lebih dikenal saat ini mulai berkembang pada tahun 1990-an bersamaan dengan munculnya *World Wide Web* (WWW). Amazon, yang didirikan pada tahun 1994 oleh Jeff Bezos, adalah salah satu perusahaan *e-commerce* pertama yang berhasil menghadirkan konsep toko buku daring yang revolusioner. Pada akhir 1990-an dan awal 2000-an, *e-commerce* mengalami pertumbuhan yang signifikan meskipun masih dalam tahap awal. Bisnis-bisnis besar dan perusahaan ritel tradisional mulai melihat potensi *e-commerce* sebagai saluran penjualan tambahan. Namun, saat itu, beberapa konsumen masih merasa ragu dan khawatir tentang keamanan transaksi online, sehingga masih banyak yang lebih memilih untuk berbelanja secara konvensional.

Perkembangan teknologi dan berbagai faktor pendorong telah berperan penting dalam memacu pertumbuhan *e-commerce* selama dua dekade terakhir. Hal ini dipicu oleh beberapa hal antara lain:

### (a) Perkembangan Infrastruktur Internet

Perluasan akses internet dan peningkatan kecepatan internet di seluruh dunia telah memfasilitasi akses lebih mudah

ke platform *e-commerce* dan mendorong pertumbuhannya;

### (b) Peningkatan Kepercayaan Konsumen

Pengamanan transaksi online dan layanan pelanggan yang lebih baik telah meningkatkan kepercayaan konsumen terhadap *e-commerce*. Review dan testimoni dari pengguna sebelumnya juga berperan penting dalam membangun kepercayaan;

### (c) Kemudahan dan Kepuasan Konsumen

*E-commerce* menawarkan kemudahan berbelanja 24/7 dari mana saja, serta beragam produk dan layanan yang dapat dipilih konsumen sesuai preferensi mereka;

### (d) Penetrasi Perangkat Seluler

Munculnya smartphone dan tablet telah mengubah cara konsumen berinteraksi dengan *e-commerce*. Transaksi melalui perangkat seluler atau *mobile commerce* telah menjadi tren utama dalam industri ini.

Seiring perkembangan *e-commerce*, industri ini mengalami segmentasi dan diversifikasi yang signifikan. Awalnya, *e-commerce* terutama terfokus pada penjualan produk fisik seperti buku, elektronik, dan pakaian. Namun, seiring waktu, *e-commerce* telah berekspansi ke berbagai sektor, termasuk travel (pemesanan tiket pesawat dan hotel), makanan dan minuman (pengantaran makanan), hiburan (*streaming* musik dan film), dan banyak lagi. Saat ini perkembangan *e-commerce* tidak lepas dari inovasi dan terobosan teknologi. Beberapa inovasi yang telah mengubah wajah *e-commerce* termasuk diantaranya yaitu:

(a) Kecerdasan Buatan (*Artificial Intelligence/ AI*)

AI telah digunakan dalam *e-commerce* untuk memberikan pengalaman berbelanja yang lebih personal, mendukung pencarian produk yang lebih akurat, dan meningkatkan layanan pelanggan;

(b) Augmented Reality (AR) dan Virtual Reality (VR)

AR dan VR telah digunakan untuk meningkatkan pengalaman berbelanja online dengan memberikan gambaran lebih nyata tentang produk dan fitur-fiturnya;

(c) Internet of Things (IoT)

IoT telah menghubungkan perangkat rumah pintar dengan *e-commerce*, memungkinkan konsumen untuk mengatur pembelian secara otomatis berdasarkan kebutuhan mereka.

Saat ini, *e-commerce* telah menjadi bagian tak terpisahkan dari revolusi digital. Banyak perusahaan *e-commerce* besar telah tumbuh pesat dan mendominasi pasar secara global. Selain itu, *e-commerce* telah memberikan kesempatan bagi banyak pelaku bisnis kecil dan menengah untuk meraih kesuksesan melalui platform daring mereka. *E-commerce* telah menjadi elemen penting dalam perekonomian berbagi (*sharing economy*), di mana platform seperti Airbnb, dan Gojek menyediakan layanan transportasi dan akomodasi berbasis daring yang mengubah cara masyarakat mengakses layanan tersebut. Namun di sisi lain, *E-commerce* tetap menghadapi berbagai tantangan, seperti meningkatkan keamanan transaksi, mengatasi permasalahan logistik dan pengiriman, serta meningkatkan perlindungan konsumen.

Permasalahan *e-commerce* yang sering terjadi adalah adanya kebocoran data konsumen dan data konsumen tersebut diperjualbelikan oleh pihak-pihak yang tidak bertanggungjawab. Kebocoran data konsumen pada *e-commerce* merupakan salah satu risiko serius yang dihadapi oleh perusahaan dan konsumen. Beberapa contoh nyata kebocoran data konsumen yang terjadi pada beberapa perusahaan *e-commerce* antara lain kebocoran Data Pengguna di eBay pada tahun 2014, situs lelang daring eBay mengalami kebocoran data yang signifikan. Hacker berhasil mengakses basis data pengguna dan mencuri informasi pribadi dari lebih dari 145 juta akun pengguna eBay, termasuk nama, alamat, nomor telepon, dan data login. Meskipun kata sandi yang diakses menggunakan enkripsi, para pelaku dapat memecahkan sebagian besar kata sandi yang lemah dengan mudah. Insiden ini mengakibatkan ketidakpercayaan konsumen terhadap eBay dan mengingatkan semua perusahaan tentang pentingnya melindungi data pribadi konsumen dengan lebih baik. Kebocoran Informasi Pembayaran di Target pada tahun 2013, jaringan toko retail Target di Amerika Serikat mengalami kebocoran data yang masif. Hacker berhasil mencuri informasi kartu kredit dan debit dari lebih dari 40 juta pelanggan Target. Serangan ini terjadi selama musim liburan, ketika aktivitas belanja mencapai puncaknya. Kebocoran data ini menyebabkan kerugian finansial yang besar bagi Target, serta merusak reputasi perusahaan sebagai tempat berbelanja yang aman. Kebocoran Informasi Pengguna di Ashley Madison, sebuah situs kencan daring yang terkenal karena menasar pasangan yang ingin berselingkuh, mengalami kebocoran

data yang memalukan pada tahun 2015. Seorang kelompok hacker yang menyebut diri mereka "The Impact Team" berhasil mencuri data dari 37 juta akun pengguna, termasuk informasi pribadi, preferensi seksual, dan pesan pribadi. Kebocoran ini menyebabkan bencana publisitas bagi situs tersebut dan menimbulkan dampak besar pada reputasi serta kepercayaan konsumen. Kebocoran Informasi Pelanggan di Home Depot pada tahun 2014, toko peralatan rumah tangga, Home Depot, menjadi korban serangan siber yang mengakibatkan kebocoran data konsumen. Hacker berhasil mencuri informasi kartu kredit dari sekitar 56 juta pelanggan yang berbelanja di toko tersebut. Serangan ini menyebabkan Home Depot mengeluarkan biaya besar untuk memperbaiki keamanan dan memperkuat perlindungan data konsumen. Kebocoran Data Pengguna di Facebook pada tahun 2018, Facebook menghadapi skandal besar ketika dilaporkan bahwa perusahaan analitik data Cambridge Analytica mengakses data pribadi dari puluhan juta pengguna Facebook tanpa izin mereka. Data ini kemudian digunakan untuk mempengaruhi pilihan politik di beberapa negara. Insiden ini menimbulkan kritik keras terhadap praktik privasi Facebook dan menyebabkan kekhawatiran tentang perlindungan data pengguna di media sosial. Kebocoran data konsumen pada e-commerce merupakan ancaman serius bagi privasi dan keamanan konsumen.

Kebocoran data pribadi konsumen juga pernah terjadi di Indonesia. Salah satu contoh kebocoran data konsumen pada e-commerce di Indonesia adalah insiden yang melibatkan situs belanja daring Bukalapak pada tahun 2020. Pada bulan Maret 2020, ditemukan bahwa data pribadi dari sekitar 13 juta akun

pengguna Bukalapak telah dijual di forum gelap daring. Informasi pribadi yang bocor meliputi nama lengkap, alamat email, nomor telepon, dan alamat pengiriman. Meskipun kata sandi akun tidak bocor dalam kasus ini, tetapi potensi penyalahgunaan data pribadi tersebut masih menjadi ancaman serius bagi para pengguna.

Insiden ini menimbulkan kekhawatiran tentang keamanan data dan privasi konsumen di e-commerce di Indonesia. Bukalapak mengambil langkah cepat untuk memberikan peringatan kepada pengguna dan menyatakan bahwa mereka telah memperkuat keamanan sistem mereka. Kasus tersebut menunjukkan betapa pentingnya bagi perusahaan e-commerce di Indonesia untuk selalu meningkatkan keamanan dan perlindungan data konsumen. Hal ini melibatkan investasi dalam sistem keamanan yang canggih, pelatihan karyawan tentang praktik keamanan data, serta transparansi dalam memberikan informasi kepada pengguna tentang bagaimana data mereka akan digunakan dan dilindungi.

Para konsumen juga harus selalu waspada terhadap potensi ancaman keamanan, seperti memastikan bahwa situs e-commerce yang mereka gunakan memiliki protokol keamanan yang tepat dan memverifikasi keaslian situs sebelum memasukkan informasi pribadi atau keuangan. Selain itu, memilih kata sandi yang kuat dan tidak menggunakan kata sandi yang sama untuk akun-akun yang berbeda juga merupakan langkah penting untuk melindungi data pribadi.

Berdasarkan latar belakang diatas, penulis tertarik membuat kajian/analisis terhadap perlindungan data pribadi konsumen pada marketplace berdasarkan peraturan

perundang-undangan yang berlaku. Secara rinci tulisan ini akan menjawab 2 (dua) permasalahan yaitu bagaimana perlindungan data pribadi konsumen dalam transaksi *e-commerce* menurut peraturan perundang-undangan yang berlaku dan bagaimana tanggung jawab *marketplace* terhadap kebocoran data pribadi konsumen.

## B. Metode Penelitian

Untuk melakukan studi mengenai perlindungan data pribadi konsumen pada transaksi *E-commerce* di Indonesia, pendekatan yang akan digunakan adalah pendekatan kualitatif dan normatif yuridis. Untuk menjawab pertanyaan permasalahan dan tujuan penelitian, metode penelitian ini adalah berupa studi literatur. Studi literatur dilaksanakan dengan melakukan kajian terhadap bahan hukum primer, sekunder dan tersier. Terkait dengan studi literatur, bahan hukum primer yang dikaji adalah peraturan perundang-undangan. Bahan hukum sekunder yang dikaji diantaranya buku, bab dalam buku, jurnal akademik, opini, laporan resmi, dan sebagainya. Sementara itu, bahan hukum tersier diantaranya adalah berupa kamus dan ensiklopedia. Teknik analisis yang digunakan dalam penelitian ini adalah teknik analisis atas interpretasi norma dan konteks dari ketentuan yang dikaji dan praktiknya di lapangan yang dikorelasikan dengan norma dalam UU PDP.

## C. Pembahasan

### 1) Pengaturan perlindungan data pribadi konsumen pada transaksi *E-commerce*

Perlindungan data pribadi konsumen menjadi isu yang semakin krusial seiring dengan meningkatnya penggunaan internet dan media sosial. Data pribadi seperti nama, alamat, nomor telepon, dan informasi lainnya yang dikumpulkan oleh berbagai platform dan penyedia layanan, menjadi sumber berharga bagi pihak-pihak tertentu. Meskipun pengumpulan data pribadi ini umumnya dimaksudkan untuk tujuan bisnis dan pemasaran yang sah, tetapi ada potensi risiko yang harus diwaspadai.

Salah satu ancaman utama adalah risiko kebocoran data atau pelanggaran keamanan yang dapat mengakibatkan data pribadi konsumen jatuh ke tangan orang yang salah. Hal ini dapat mengakibatkan pencurian identitas, penipuan, dan eksploitasi lainnya. Kebocoran data juga dapat menyebabkan kerugian finansial dan kerugian reputasi bagi individu dan perusahaan yang terlibat. Oleh karena itu, perlindungan data pribadi konsumen menjadi sangat penting dan mendesak. Pengaturan perlindungan data pribadi konsumen pada transaksi *e-commerce* berperan dalam mengatur pengumpulan, penggunaan, penyimpanan, dan perlindungan data pribadi oleh perusahaan dan platform *e-commerce*. Tujuan dari pengaturan ini adalah untuk melindungi privasi, keamanan, dan hak-hak konsumen dalam penggunaan data pribadi mereka.

Terkait dengan perlindungan hukum, Isnaeni<sup>1</sup> mengatakan bahwa berdasarkan

<sup>1</sup> Isnaeni. Moch, *Seberkas Diaroma Hukum Kontrak* (Surabaya: PT Revka Petra Media, 2017), hlm. 159

sumbernya perlindungan hukum dapat dibagi menjadi 2 (dua) jenis yaitu perlindungan internal dan perlindungan eksternal. Perlindungan hukum internal dapat diwujudkan oleh para pihak, disaat kedudukan hukum antara kedua pihak relatif seimbang, artinya mereka memiliki *bargaining power* yang berimbang, sehingga atas dasar hak asasi manusia, para pihak mempunyai keleluasaan untuk menyatakan kehendak sesuai kepentingannya. Hal ini menjadi landasan saat para pihak menyusun klausul-klausul kesepakatan, sehingga perlindungan hukum dapat terwujud sesuai kebutuhan para pihak. Perlindungan hukum eksternal yang dibuat oleh penguasa lewat regulasi dapat memberikan perlindungan bagi kepentingan pihak yang lemah. Hakekat peraturan perundang-undangan harus seimbang dan tidak boleh berat sebelah. Secara proporsional juga wajib diberikan perlindungan hukum yang seimbang sedini mungkin kepada pihak lainnya. Sebab mungkin saja pada saat dibuatnya sebuah kesepakatan, pihak yang semula kuat itu justru menjadi pihak yang teraniaya. Misalnya, saat debitur melanggar hak kreditur, maka kreditur perlu perlindungan hukum juga. Kemasam peraturan perundang-undangan memberikan perlindungan hukum kepada para pihak secara proporsional.<sup>2</sup>

Perlindungan hukum merupakan suatu hal yang dilindungi sebagai subyek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan adanya sanksi yang diberikan. Perlindungan hukum dapat dibedakan menjadi dua, yaitu perlindungan preventif dan represif.

Muchsin<sup>3</sup> mengatakan bahwa perlindungan yang diberikan oleh pemerintah bertujuan untuk mencegah sebelum terjadinya suatu pelanggaran. Hal ini terdapat di dalam peraturan perundang-undangan yang bertujuan untuk mencegah terjadinya akan suatu pelanggaran dan dapat memberikan batasan dalam melakukan suatu kewajiban. Pada perlindungan hukum preventif ini, subyek hukum diberikan kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Tujuannya adalah mencegah terjadinya sengketa. Perlindungan hukum preventif sangat besar artinya bagi tindak pemerintahan yang didasarkan pada kebebasan bertindak karena dengan adanya perlindungan hukum yang preventif pemerintah terdorong untuk lebih bersifat hati-hati dalam mengambil keputusan yang didasarkan pada diskresi.

Sedangkan perlindungan represif, CST Kansil<sup>4</sup> mengatakan bahwa perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran hukum. Perlindungan hukum represif bertujuan untuk menyelesaikan suatu sengketa. Penanganan perlindungan hukum oleh Pengadilan Umum dan Pengadilan Administrasi di Indonesia termasuk kategori perlindungan hukum ini. Prinsip perlindungan hukum terhadap tindakan pemerintah bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia karena menurut sejarah dari barat,

<sup>2</sup> Ibid.

<sup>3</sup> Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia* (Surakarta: Universitas Sebelas Maret, 2003), hlm. 14

<sup>4</sup> CST Kansil, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia* (Jakarta: Balai Pustaka, 1989), hlm. 102.

lahirnya konsep-konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia diarahkan kepada pembatasan-pembatasan dan peletakan kewajiban masyarakat dan pemerintah. Prinsip kedua yang mendasari perlindungan hukum terhadap tindak pemerintahan adalah prinsip negara hukum. Dikaitkan dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia mendapat tempat utama dan dapat dikaitkan dengan tujuan negara hukum.

Dengan demikian perlindungan hukum dimaksudkan sebagai perlindungan yang diberikan oleh negara kepada setiap warga negara yang dirugikan hak-haknya. Perlindungan hukum merupakan dasar dari sistem hukum yang berkeadilan dan dapat menciptakan kerangka kerja untuk menyelesaikan konflik, mempertahankan hak-hak individu dan menjaga ketertiban sosial. Hal ini penting untuk memastikan bahwa pemerintah dan pihak berwenang tidak dapat bertindak sewenang-wenang terhadap warga negara. Perlindungan hukum melibatkan proses hukum yang adil, akses terhadap pengadilan dan penerapan hukum yang sama terhadap semua orang.

Dalam konteks perlindungan data pribadi konsumen, peraturan perundang-undangan memainkan peran kunci. Perlindungan data pribadi selayaknya mendapat perlindungan dari pemerintah dimana hal tersebut berhubungan dengan data pribadi yang merupakan hak asasi warga negara. Di Indonesia sendiri, Undang-Undang Dasar

Negara Republik Indonesia Tahun 1945 telah mengakui adanya hak terhadap perlindungan data pribadi warga negaranya yang tercantum dalam Pasal 28 huruf G yaitu setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Pasal tersebut secara jelas menyatakan bahwa negara menjamin hak dan perlindungan pribadi warga negaranya. Mahkamah Konstitusi mempertahankan hak atas privasi sebagai bagian dari perlindungan data pribadi dalam Putusan Nomor 20/PUU-XIV/2016. Namun, perlindungan data dan privasi adalah dua konsep yang berbeda. Hak atas perlindungan data pribadi adalah hak asasi manusia dan termasuk dalam hak privasi, termasuk privasi informasi dan privasi data, menurut Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2011. Hak privasi juga dilindungi oleh perjanjian hukum internasional sebagai hak asasi manusia. Pelanggan harus memberikan informasi pribadi seperti nama lengkap, nomor telepon, dan detail lain yang relevan untuk mendaftar di platform *e-commerce*. Pelanggan mungkin diminta untuk mengunggah foto kartu identitas (Kartu Tanda Penduduk/KTP), foto selfie dengan KTP, atau tanda tangan digital dalam situasi tertentu. Komponen-komponen data pribadi ini perlu dilindungi. Pemerintah memainkan peran penting dalam menerbitkan kebijakan yang dapat membantu melindungi data pribadi.<sup>5</sup>

<sup>5</sup> Tia Deja Pohan dan Muhammad Irwan Padli Nasution, "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce", Jurnal Penelitian Bisnis dan Manajemen Vol.1, No.3 September 2023, hlm. 5

Kesadaran masyarakat akan perlindungan data pribadi yang dimilikinya atau hak privasi juga menjadi tanggung jawab negara dalam memberikan edukasi atau pengetahuan yang setara dan merata bagi setiap masyarakatnya. Karena bila hak privasi tidak dilindungi maka dapat mengancam keselamatan jiwa maupun materiil. Selain memberikan edukasi, tentunya Indonesia sebagai negara harus memberikan perlindungan hukum terhadap warga negaranya berdasarkan atas sesuai dengan Pancasila.<sup>6</sup>

Pada awalnya Indonesia tidak memiliki aturan khusus yang mengatur perlindungan data pribadi. Perlindungan data pribadi hanya diatur secara umum pada beberapa peraturan perundang-undangan yang terpisah seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informatika dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan Pokok Kearsipan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 36 Tentang Telekomunikasi dan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Selain itu terdapat undang-undang yang secara khusus memberikan perlindungan terhadap konsumen yaitu Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Pada tahun 2022, Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini diterbitkan atas dasar kebutuhan untuk melindungi privasi individu dan menjaga keamanan data pribadi dalam era digital yang semakin berkembang. Latar belakang utama untuk regulasi ini adalah perkembangan pesat teknologi informasi dan komunikasi yang telah mengubah cara kita mengumpulkan, menyimpan, mengolah, dan mentransfer data pribadi. Pengaturan mengenai perlindungan data pribadi diharapkan akan menempatkan Indonesia sejajar dengan negara-negara maju yang telah menerapkan hukum mengenai perlindungan data pribadi. Hal ini akan lebih mendorong dan memperkuat posisi Indonesia sebagai pusat bisnis terpercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia.<sup>7</sup>

Salah satu tonggak penting dalam mendukung peraturan perlindungan data pribadi ini adalah berkat kehadiran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE memberikan dasar hukum untuk melindungi privasi individu dalam lingkungan digital dan memberikan sanksi terhadap tindakan penyalahgunaan data. UU ITE memiliki ketentuan yang mengatur tentang perlindungan data pribadi dalam transaksi elektronik sebagaimana diatur di dalam ketentuan Pasal 25 dan Pasal 26 UU ITE.

Pasal 25 UU ITE menyebutkan bahwa Informasi Elektronik dan/atau Dokumen

<sup>6</sup> Rizal, M.S., "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum*, 10 (2), 2019, hlm. 39-42

<sup>7</sup> Enny Nurbaningsih, dkk, "Naskah Akademik Rancangan Undang-Undang Perlindungan Data Pribadi", BPHN, 2016

Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan intelektual berdasarkan ketentuan Peraturan Perundang-undangan. Sedangkan Pasal 26 UU ITE mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.<sup>8</sup> Dalam penjelasannya, Pasal 26 UU ITE menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut: a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai. c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Bila ditarik penafsiran secara umum, maka perlindungan data pribadi sebenarnya telah diatur di dalam UU ITE. Pasal-Pasal selanjutnya dalam UU ITE yaitu Pasal 30-33 dan Pasal 35 yang masuk kedalam BAB VII mengenai Perbuatan yang Dilarang. Secara tegas, Undang-Undang ITE melarang adanya akses secara melawan hukum kepada data pribadi milik orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengamanan. Selain itu juga UU ITE menyatakan bahwa

penyadapan (*interception*) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam rangka upaya hukum. Setiap orang yang merasa dirugikan akibat dilakukannya perbuatan yang dilarang tersebut dapat mengajukan gugatan ganti kerugian, dan pelaku pun mempunyai tanggung gugat atas apa yang dilakukannya.

UU ITE telah memberikan perlindungan terhadap data pribadi dalam transaksi elektronik namun tidak memberikan pengaturan secara rinci apa yang dimaksud dengan data pribadi. Pengertian data pribadi dapat ditemukan dalam beberapa peraturan di bawah UU ITE seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Elektronik. Selain itu pengertian data pribadi juga dapat ditemukan di dalam UU PDP.

UU PDP mengatur apa saja yang termasuk data pribadi. Berdasarkan Pasal 4 Undang-Undang tersebut ada dua jenis data pribadi, berikut ini jenis-jenis data pribadi, yaitu:<sup>9</sup>

1. Data pribadi yang bersifat spesifik, meliputi:
  - a) Data dan informasi kesehatan;
  - b) Data biometrik;
  - c) Data genetika;
  - d) Catatan kejahatan;
  - e) Data anak;
  - f) Data keuangan pribadi;
  - g) Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
2. Data pribadi yang bersifat umum, meliputi:

<sup>8</sup> Liat Pasal 26 Undang-Undang Nomor 11 Tahun 2008 tentang Informatika dan Transaksi Elektronik

<sup>9</sup> Lihat Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

- a) Nama lengkap;
- b) Jenis kelamin;
- c) Kewarganegaraan;
- d) Agama;
- e) Status perkawinan;
- f) Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Pelindungan Data Pribadi pada dasarnya merupakan ketentuan yang memberikan standar Pelindungan Data Pribadi secara umum, baik yang diproses sebagian atau keseluruhan dengan cara elektronik dan nonelektronik, dimana masing-masing sektor dapat menerapkan Pelindungan Data Pribadi sesuai karakteristik sektor yang bersangkutan. Pengaturan Data Pribadi bertujuan antara lain melindungi dan menjamin hak dasar warga negara terkait dengan pelindungan diri pribadi, menjamin masyarakat untuk mendapatkan pelayanan dari Korporasi, Badan Publik, Organisasi Internasional, dan Pemerintah, mendorong pertumbuhan ekonomi digital dan industri teknologi informasi dan komunikasi, dan mendukung peningkatan daya saing industri dalam negeri.<sup>10</sup>

Perlindungan data pribadi dalam transaksi e-commerce juga telah diatur di dalam Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) khususnya diatur di dalam Pasal 58-59.

Pasal 58 PP PMSE menyebutkan bahwa:

- 1) Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau Pelaku Usaha yang bersangkutan.
- 2) Setiap Pelaku Usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengemban

amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan.

Dalam ketentuan Pasal 58 – 59 PP PMSE hanya mengatur amanah kepada pelaku usaha untuk mengelola data pribadi milik masyarakat tanpa adanya regulasi terkait sanksi atau tanggung jawab bilamana terjadi kegagalan dalam perlindungan data pribadi.

Dari perspektif yuridis, konsep data pribadi sebagai hak milik menegaskan bahwa individu atau Pelaku Usaha memiliki kontrol penuh atas data pribadi mereka, termasuk hak untuk mengizinkan atau menolak penggunaan dan pengungkapan data tersebut oleh pihak lain. Pengakuan data pribadi sebagai hak milik dapat melindungi privasi dan keamanan informasi individu atau Pelaku Usaha. Ketentuan tersebut juga mencerminkan asas hukum tentang hak milik, yaitu prinsip yang menyatakan bahwa setiap orang memiliki hak eksklusif atas kepemilikan dan penggunaan benda atau aset miliknya. Asas hak milik ini mendorong perlindungan terhadap hak kepemilikan individu atau Pelaku Usaha atas data pribadi mereka, sehingga pihak lain tidak dapat menggunakan data tersebut tanpa izin atau tanpa tujuan yang sah.

Dilihat dari perspektif filosofis, pemahaman bahwa data pribadi merupakan hak milik individu atau Pelaku Usaha menegaskan nilai-nilai kemandirian, otonomi, dan martabat manusia. Pengakuan ini menegaskan bahwa individu atau Pelaku Usaha memiliki kendali atas data pribadi mereka dan memiliki hak untuk melindungi kehidupan pribadi dan identitas mereka dari penggunaan yang tidak sah.

<sup>10</sup> Penjelasan umum, ibid.

Perlindungan Data Pribadi Konsumen Dalam Transaksi Elektronik juga diatur di dalam Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Peraturan Kominfo 20/2016). Secara garis besar peraturan ini berisi:

1. Definisi Data Pribadi

Peraturan Kominfo 20/2016 memberikan definisi tentang apa yang dimaksud dengan data pribadi. Data pribadi diartikan sebagai segala informasi mengenai individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik sendiri atau dengan menghubungkannya dengan informasi lain. Definisi ini mencakup segala jenis informasi, termasuk nama, alamat, nomor telepon, alamat email, nomor identitas, riwayat transaksi, dan informasi lain yang berhubungan dengan individu.

2. Hak Pribadi atas Data Pribadi

Peraturan Kominfo 20/2016 mengakui hak pribadi individu atas data pribadi mereka. Konsumen memiliki hak untuk mengetahui, mengakses, mengoreksi, menghapus, membatasi penggunaan, dan memindahkan data pribadi mereka yang dikelola oleh pihak lain. Konsumen juga berhak untuk mengajukan keluhan atau protes jika data pribadi mereka digunakan secara tidak sah atau melanggar ketentuan peraturan ini.

3. Kewajiban Pengelola Data Pribadi

Peraturan Kominfo 20/2016 menetapkan kewajiban bagi pengelola data pribadi, yaitu pihak yang mengumpulkan, mengolah, menyimpan, dan mengelola data pribadi. Pengelola data pribadi harus mengikuti prinsip keadilan, transparansi, keterbatasan tujuan, ketepatan,

kemanfaatan, akurasi, keamanan, dan tanggung jawab dalam mengelola data pribadi konsumen.

4. Persyaratan Penyimpanan dan Penggunaan Data Pribadi

Peraturan Kominfo 20/2016 menetapkan persyaratan tentang penyimpanan dan penggunaan data pribadi. Data pribadi harus disimpan dalam batas waktu yang wajar sesuai dengan tujuan pengumpulan data tersebut. Pengelola data pribadi juga harus memastikan keamanan data pribadi dari akses, penggunaan, dan pengungkapan yang tidak sah.

5. Notifikasi Pelanggaran Data

Peraturan Kominfo 20/2016 mewajibkan pengelola data pribadi untuk memberikan notifikasi kepada konsumen jika terjadi pelanggaran keamanan yang mengakibatkan akses, penggunaan, atau pengungkapan data pribadi yang tidak sah. Notifikasi tersebut harus dilakukan sesegera mungkin agar konsumen dapat mengambil langkah-langkah untuk melindungi diri mereka dari potensi penyalahgunaan data.

6. Penggunaan Data Pribadi untuk Pemasaran

Peraturan Kominfo 20/2016 mengatur tentang penggunaan data pribadi untuk kepentingan pemasaran. Pengelola data pribadi harus mendapatkan izin atau persetujuan dari konsumen sebelum menggunakan data pribadi untuk tujuan pemasaran, kecuali jika ada ketentuan hukum yang mengizinkan penggunaan data pribadi tanpa izin.

7. Pengalihan Data Pribadi

Peraturan Kominfo 20/2016 mengatur tentang pengalihan data pribadi ke pihak ketiga. Pengalihan data pribadi ke pihak

ketiga hanya dapat dilakukan dengan persetujuan tertulis dari konsumen, kecuali jika ada ketentuan hukum atau peraturan yang mengizinkan pengalihan data pribadi.

#### 8. Penghapusan Data Pribadi

Peraturan Koinfo 20/2016 menetapkan kewajiban untuk menghapus data pribadi konsumen jika tujuan pengumpulan data tersebut telah tercapai atau data pribadi tidak diperlukan lagi untuk tujuan yang sah. Penghapusan data pribadi harus dilakukan secara aman dan terjamin.

Perlindungan data pribadi konsumen dalam penyelenggara sistem elektronik dilakukan dengan membuat *code of conduct* berupa *self-regulation* (kebijakan internal). Bagi perusahaan yang bergerak dalam perdagangan secara elektronik, *self-regulation* dalam bentuk *privacy policy* merupakan salah satu alternatif yang paling mungkin untuk memecahkan persoalan perlindungan data pribadi konsumen. Hal ini merupakan amanat Pasal 5 ayat (2) Peraturan Koinfo 20/2016 menyebutkan bahwa "Setiap Penyelenggara Sistem Elektronik harus menyusun aturan internal perlindungan Data Pribadi sebagai bentuk tindakan pencegahan untuk menghindari terjadinya kegagalan dalam perlindungan Data Pribadi yang dikelolanya."<sup>11</sup>

Jauh sebelum adanya UU ITE dan UU PDP, Negara juga telah memberikan perlindungan kepada konsumen melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU PK). Di dalam UU PK telah

diatur hak dan kewajiban konsumen. Di dalam Pasal 4 UU PK disebutkan mengenai hak-hak konsumen. Salah satu hak konsumen adalah "hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa".<sup>12</sup> Hal ini berarti dalam setiap transaksi jual beli konsumen berhak mendapatkan kenyamanan dan keamanan terhadap data pribadinya. Selanjutnya di dalam Pasal 7 UU PK terdapat kewajiban pelaku usaha. Salah satu kewajiban pelaku usaha adalah beritikad baik. Dengan demikian apabila dalam transaksi elektronik sebelum terjadinya transaksi, penjual meminta data pribadi konsumen seperti alamat, no hp dll maka penjual wajib dengan itikad baik menjaga kerahasiaan data pribadi konsumen dan tidak menyebarkan untuk hal-hal yang tidak baik.

Jika konsumen merasa dirugikan maka konsumen dapat mengajukan gugatan berdasarkan Pasal 45 UU PK. Pasal 45 UU PK menyebutkan bahwa "Setiap konsumen yang dirugikan dapat menggugat pelaku usaha melalui lembaga yang bertugas menyelesaikan sengketa antara konsumen dan pelaku usaha atau melalui peradilan yang berada di lingkungan peradilan umum". Kemudian untuk penyelesaian sengketanya, konsumen dapat memilih melalui pengadilan ataupun melalui jalur di luar pengadilan.

Kasus yang pernah terjadi pada kebocoran data pribadi pada platform Tokopedia yang kemudian berujung diajukan gugatan oleh David Tobing. David menilai bahwa Menkominfo telah lalai dalam

<sup>11</sup> Josephine, et all, "Perlindungan Konsumen Daring Dan Tanggung Jawab Perusahaan Marketplace Atas Data Privasi Konsumen", Suara Keadilan, Vol. 21 No. 1, April 2020, Halaman 97-112 p-ISSN: 1829-684X, e-ISSN: 2621-9174, hlm. 105

<sup>12</sup> Lihat Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999.

melakukan pengawasan penyelenggaraan sistem elektronik oleh Tokopedia sehingga mengakibatkan data pribadi pemilik akun Tokopedia diretas oleh pihak yang tidak bertanggungjawab secara melawan hukum.

## 2) Tanggung Jawab *Market Place* terhadap Data Pribadi Konsumen

Tanggung jawab *market place* terhadap konsumen sangat penting untuk memastikan perlindungan hak dan kepentingan konsumen dalam transaksi *e-commerce*. Sebagai platform atau tempat transaksi online, *market place* memiliki peran yang signifikan dalam memfasilitasi pertemuan antara penjual dan konsumen. Berikut adalah beberapa tanggung jawab *market place* terhadap konsumen:

### a) Keamanan Data Pribadi

*Market place* harus menjaga keamanan data pribadi konsumen yang terdaftar di platformnya. Hal ini mencakup pengumpulan, penggunaan, dan pengolahan data pribadi dengan itikad baik dan sesuai dengan peraturan perundang-undangan yang berlaku. *Market place* harus melindungi informasi pribadi konsumen dari akses yang tidak sah dan memastikan bahwa data tersebut tidak digunakan untuk tujuan yang tidak sah.

### b) Ketersediaan dan Keandalan Produk/ layanan

*Market place* bertanggung jawab untuk memastikan ketersediaan dan keandalan produk atau layanan yang ditawarkan oleh penjual kepada konsumen. *Market place* harus memverifikasi kredibilitas penjual dan menghapus penjual yang terbukti menjual produk palsu atau melakukan praktik penipuan.

### c) Transparansi Informasi

*Market place* harus menyediakan informasi yang jelas dan akurat tentang produk atau layanan yang ditawarkan. Informasi seperti harga, deskripsi produk, persyaratan pengiriman, dan kebijakan pengembalian harus tersedia secara transparan untuk membantu konsumen membuat keputusan pembelian yang tepat.

### d) Penanganan Perselisihan

*Market place* harus memiliki mekanisme penanganan perselisihan yang efektif antara konsumen dan penjual. Jika terjadi masalah dalam transaksi, *market place* harus berperan sebagai mediator untuk membantu mencari solusi yang adil bagi kedua belah pihak.

### e) Kebijakan Pengembalian dan Jaminan Kualitas

*Market place* harus memiliki kebijakan pengembalian yang jelas dan adil bagi konsumen jika produk atau layanan yang diterima tidak sesuai dengan harapan atau rusak. Selain itu, *market place* juga harus menjamin kualitas produk atau layanan yang ditawarkan agar konsumen merasa aman melakukan transaksi.

### f) Perlindungan Konsumen terhadap Praktik Penipuan

*Market place* harus aktif dalam melawan praktik penipuan dan produk palsu. Penjual yang terlibat dalam praktik penipuan harus dihapus dari platform dan pencegahan harus dilakukan untuk mencegah penipuan yang serupa.

### g) Edukasi Konsumen

*Market place* juga memiliki tanggung jawab untuk mengedukasi konsumen tentang hak dan kewajiban mereka dalam bertransaksi

online. Edukasi ini dapat berupa informasi tentang cara melindungi diri dari penipuan, cara melaporkan praktik curang, dan hak-hak dalam transaksi *e-commerce*.

Secara umum pertanggungjawaban memiliki arti keadaan wajib menanggung segala perbuatan yang dilakukan. Konsep pertanggungjawaban secara hukum atas tindakan yang dilakukan oleh seseorang atau kelompok yang bertentangan dengan Undang-undang. Menurut kamus hukum "Tanggung jawab adalah suatu keharusan bagi seseorang untuk melaksanakan dengan selayaknya apa yang telah diwajibkan kepadanya".<sup>13</sup> Hans Kelsen, seorang ahli hukum dan filsuf hukum terkenal dari Austria, yang dikenal dengan kontribusinya dalam teori hukum positivisme dan teori hukum murni, mengatakan bahwa pertanggungjawaban atau tanggung jawab dalam konteks hukum didasarkan pada norma hukum yang berlaku. Lebih lanjut ia mengatakan seseorang bertanggung jawab secara hukum atas perbuatan yang dilakukannya. Dalam konteks terjadi kebocoran data pribadi konsumen, terdapat beberapa prinsip pertanggungjawaban yang dapat diterapkan kepada *market place* yaitu:

a) Prinsip berdasarkan kesalahan (*Liability based on Fault*)

Yang dimaksud kesalahan adalah unsur yang bertentangan dengan hukum. Pengertian hukum tidak hanya bertentangan dengan undang-undang tetapi juga kepatutan dan kesusilaan dalam masyarakat. Untuk itu prinsip yang didasarkan pada kesalahan

harus dibuktikan bahwa adanya hubungan antara kesalahan dan kerugian.

b) Prinsip Praduga untuk selalu bertanggung jawab (*Presumption of Liability principle*) Prinsip praduga untuk selalu bertanggung jawab menyatakan bahwa pihak yang menjadi tergugat selalu dianggap bertanggung jawab (*presumption of liability principle*), sampai si tergugat dapat membuktikan bahwa dirinya tidak bersalah.<sup>14</sup>

Secara umum prinsip ini menyatakan bahwa tergugat (dalam hal ini *market place*) dianggap selalu bertanggung jawab sampai ia dapat membuktikan bahwa dirinya tidak bersalah dan beban pembuktian ada pada tergugat.<sup>15</sup> Pembuktian semacam ini juga dikenal sebagai sistem pembuktian terbalik. Konstruksi praduga untuk selalu bertanggung jawab dalam menanggapi kasus kebocoran data yang terjadi dapat dianggap relevan ketika suatu kebocoran data merupakan *force majeure* atau akibat kelalaian pihak online *marketplace*.

c) Prinsip Tanggung Jawab Mutlak (*strict liability*)

Prinsip tanggung Jawab Mutlak (*strict liability/absolute liability*) yaitu bahwa pihak yang menimbulkan kerugian (tergugat) selalu bertanggung jawab tanpa melihat ada atau tidaknya kesalahan atau tidak melihat siapa yang bersalah. Menurut Sidharta, *Strict liability* merupakan wujud distingtif dari suatu perbuatan melawan hukum yaitu prinsip pertanggungjawaban dalam perbuatan melawan hukum

<sup>13</sup> Andi Hamzah, Kamus Hukum (Jakarta: Ghalia Indonesia, 1986), hlm.570

<sup>14</sup> Shidarta, Hukum Perlindungan Konsumen Indonesia (Jakarta: PT Grasindo, 2000), hlm. 59.

<sup>15</sup> Aulia Muthiah, "Tanggung Jawab Pelaku Usaha Kepada Konsumen tentang Keamanan Pangan dalam Perspektif Hukum Perlindungan Konsumen", *Dialogia Iuridica: Jurnal Hukum Bisnis dan Invetasi*, Volume 7, Nomor 2, 2016, hlm.9

yang tidak didasarkan pada kesalahan pada umumnya, melainkan prinsip ini mengharuskan para pelaku usaha untuk langsung bertanggung jawab atas kerugian yang timbul karena perbuatan melawan hukum itu.<sup>16</sup> Dengan demikian *market place* tidak bertanggung jawab atas kebocoran data pribadi konsumen jika kebocoran data tersebut disebabkan karena suatu keadaan memaksa. Hal ini selaras dengan pendapat beberapa ahli yang menafsirkan *strict liability* sebagai tanggung jawab yang menentukan kesalahan tidak sebagai faktor yang pasti, namun terdapat pengecualian yaitu suatu *force majeure*.<sup>17</sup>

Jika dilihat dari ketentuan Pasal 15 ayat (1) UU ITE disebutkan bahwa:

- (1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
- (2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

Namun pasal 15 UU ITE ini menjadi tidak berlaku jika *marketplace* dapat membuktikan adanya keadaan memaksa dan atau adanya kesalahan/kelalaian pihak pengguna sistem elektronik. Dalam beberapa kasus kebocoran data pribadi pada *marketplace*, menunjukkan

adanya kelemahan pada sistem pengamanan dalam sistem elektronik pada *market place* tersebut sehingga menyebabkan dapat diaksesnya data-data konsumen yang ada pada *marketplace* tersebut. Kejadian tersebut menunjukkan kurang andal dan amannya sistem elektronik yang dimiliki oleh *marketplace* sehingga dapat dengan mudah dilakukan peretasan hingga data pribadi penggunanya bocor dan dijual pada situs web gelap. Hal ini bertentangan dengan ketentuan Pasal 15 UU ITE juga Pasal 3 PP PSE yang memberikan kewajiban pada Penyelenggara Sistem Elektronik untuk menyelenggarakan Sistem Elektroniknya secara andal dan aman. Berdasarkan ketentuan tersebut maka tanggung jawab atas kebocoran data pribadi pengguna marketplace merupakan tanggung jawab dari penyelenggara *marketplace*.

Jika dilihat dari ketentuan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), Penyelenggara Sistem Elektronik bahwa “Penyelenggara Sistem Elektronik wajib melindungi penggunanya dan masyarakat luas dari kerugian yang ditimbulkan oleh Sistem Elektronik yang diselenggarakannya”,<sup>18</sup> dan Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan.<sup>19</sup> Selanjutnya di dalam

<sup>16</sup> Sidharta, op. cit. hlm. 63

<sup>17</sup> Putu Ari Sara Deviyanti, “Tuntutan Ganti Rugi Penggunaan Data Pribadi Surat Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik”, Skripsi, Fakultas Hukum Udayana, 2017, hlm. 21-22

<sup>18</sup> Lihat Pasal 31 PP 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

<sup>19</sup> Ibid, Pasal 26

Pasal 14 ayat (5) PP 71/2019 disebutkan jika terjadi kegagalan dalam perlindungan terhadap Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut. Dalam arti jika terjadi peretasan terhadap server yang menyimpan data pribadi penyelenggara wajib memberitahukan kepada pihak-pihak. Dengan demikian penyelenggara sistem elektronik wajib melindungi data-data yang tersimpan namun kadang-kadang ada oknum yang menyebarkan data pribadi tersebut secara tidak bertanggung jawab. Oleh karenanya penyelenggara sistem elektronik juga mempunyai kewajiban untuk mendidik personal yang bertugas untuk bertanggung jawab terhadap pengamanan dan perlindungan sarana dan prasarana dalam arti penyelenggara sistem elektronik mendidik personal yang bertugas untuk melindungi sarana dalam sistem elektronik misalnya program komputer yang berisi data pribadi individu harus selalu diamankan.

Selanjutnya jika dilihat dari ketentuan UU PDP terdapat pasal-pasal yang memberikan kewajiban kepada Pengendali data pribadi. Pengendali data pribadi menurut UU PDP adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.<sup>20</sup> Pengendali data pribadi disini bisa Pemerintah maupun swasta. Dari Pemerintah misalnya adalah Direktorat Jenderal Kependudukan dan Pencatatan Sipil, Kementerian Dalam Negeri yang mencatat data pribadi penduduk untuk kepentingan

negara maupun publik. Sementara dari pihak swasta, *marketplace* bisa menjadi salah satu contohnya. Sebab, untuk dapat menggunakan atau mengakses semua layanan yang diberikan, masyarakat harus memasukan data pribadinya.<sup>21</sup>

Pasal 35 UU PDP menyebutkan bahwa Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan dan penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.

Kemudian Pasal 39 UU PDP menyebutkan bahwa:

- (1) Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah;
- (2) Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi sistem elektronik secara andal, aman, dan bertanggung jawab.
- (3) Pencegahan sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

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

<sup>20</sup> Lihat Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

<sup>21</sup> <https://www.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel, diakses pada tanggal 10 Juli 2023>

- (2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat: Data Pribadi yang terungkap; kapan dan bagaimana Data Pribadi terungkap; dan upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.

Dari ketentuan di atas terlihat adanya kewajiban *marketplace* untuk melindungi data pribadi. Namun jika terjadi kebocoran data pribadi maka *marketplace* sebagai pengendali data pribadi wajib memberitahukan kepada konsumen yang datanya diretas oleh pihak yang tidak bertanggung jawab. Selain itu, *marketplace* dapat dikenakan sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi, dan/atau denda administratif sebagaimana diatur di dalam Pasal 57 UU PDP. Demikian pula berdasarkan ketentuan di dalam PP 71 Tahun 2019, Penyelenggara Sistem elektronik juga dapat dikenakan sanksi berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan Akses, dan/atau dikeluarkan dari daftar.<sup>22</sup>

Dalam hal terjadi kebocoran data pribadi konsumen, maka konsumen dapat mengajukan pengaduan ke Menteri atas kegagalan perlindungan kerahasiaan data pribadi, pasal ini memiliki hubungan dengan Pasal 26 huruf b yang menyebutkan pemilik data berhak melakukan pengaduan kepada Menteri atas kegagalan perlindungan data pribadi.<sup>23</sup>

Selain itu konsumen sebagai pihak yang dirugikan dapat mengajukan gugatan secara

perdata kepada *marketplace* dengan alasan adanya unsur kelalaian dari *marketplace*. Dalam kaitannya dengan unsur kelalaian, Pasal 1336 KUH Perdata menyebutkan bahwa setiap orang bertanggung jawab, bukan hanya atas kerugian yang disebabkan perbuatan-perbuatan, melainkan juga atas kerugian yang disebabkan kelalaian atau kesembronannya.

Dari ketentuan Pasal 1366 KUHPerdata tersebut mengandung pengertian bahwa seseorang dapat mempunyai tanggung jawab secara hukum bukan hanya atas kerugian yang disebabkan oleh kesalahan yang dia perbuat tetapi juga atas kelalaiannya yang menimbulkan kerugian bagi orang lain.

Berdasarkan Pasal 64 UU PDP, penyelesaian sengketa dapat dilakukan melalui arbitrase, pengadilan atau Lembaga penyelesaian sengketa alternatif dengan menggunakan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan dengan dilengkapi alat bukti yang sah.

#### D. Penutup

Sebelum tahun 2022, pengaturan perlindungan data pribadi diatur dalam beberapa peraturan perundang-undangan yang tersebar namun saat ini Indonesia telah memiliki undang-undang yang secara khusus memberikan perlindungan terhadap data pribadi. Pentingnya menjamin hak konsumen *e-commerce* di Indonesia sendiri dikarenakan permasalahan data pribadi sudah menjadi hal yang serius dan harus segera diatasi. Hal tersebut juga didukung dengan banyak kasus kebocoran data pribadi di Indonesia

<sup>22</sup> Lihat Pasal 100 ayat (2) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

<sup>23</sup> Lihat Pasal 26 huruf b, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik tentang Penyelenggaraan Sistem dan Transaksi Elektronik

di beberapa platform *e-commerce*. Hal tersebut menjadi suatu ancaman besar bagi Pemerintah ketika tidak dapat melindungi hak konsumen *e-commerce*.

Jika terjadi kebocoran data pribadi konsumen, maka *marketplace* sebagai pengendali data pribadi wajib bertanggung jawab atas kerugian yang dialami oleh konsumen. Selain itu konsumen sebagai subyek data pribadi dapat mengajukan gugatan ganti rugi atas dasar kelalaian *marketplace* berdasarkan Pasal 1366 KUH Perdata.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengamanatkan dibentuknya Lembaga pengawas perlindungan data pribadi. Lembaga tersebut mempunyai peranan yang sangat penting dalam pengawasan terhadap pemyelenggaraan perlindungan data pribadi. Lembaga tersebut juga dapat dimanfaatkan oleh konsumen untuk mengadu atau menyalurkan aspirasinya terkait dengan perlindungan data pribadi. Mengingat peran Lembaga tersebut sangat penting, Pemerintah perlu segera membentuk Lembaga tersebut yang bersifat independent. Selain itu agar konsumen selalu menjaga data pribadinya perlu dilakukan edukasi literasi digital kepada masyarakat tentang pentingnya menjaga data pribadi.

## DAFTAR PUSTAKA

### Buku-buku

- Assiddiqi Jimly dan Ali Safa'at, *Teori Hans Kelsen tentang Hukum*, (Jakarta: Sekretariat Jenderal &Kepaniteraan Mahkamah Konstitusi, 2006)
- Gulton, Elistaris. *Cyber Law: Suatu Pengantar Perlindungan Konsumen Dalam Transaksi Perdagangan Melalui Electronic Commerce*. Elips. Bandung.

- Halim Barkatullah Abdul dan Teguh Prasetyo, *Bisnis E-Commerce*, (Yogyakarta: Pustaka Pelajar, 2005)
- Hamzah, Andi, *Kamus Hukum*, (Jakarta: Ghalia Indonesia, 1986)
- Indrajit, Richardus Eko, *Kiat dan Strategi Bisnis di Dunia Maya*, (Jakarta: PT. Elex Media Komputindo, 2001)
- Isnaeni. Moch, *Seberkas Diaroma Hukum Kontrak*. (Surabaya:PT Revka Petra Media, 2018)
- Kansil, CST, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, (Jakarta: Balai Pustaka, 1989)
- Muchsin. 2003. *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, (Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret
- Shidarta, *Hukum Perlindungan Konsumen Indonesia*, (Jakarta: PT Grasindo, 2006), cetakan ketiga

### Jurnal/Hasil Penelitian/Skripsi

- Enny Nurbaningsih, dkk, "Naskah Akademik Rancangan Undang-Undang Perlindungan Data Pribadi", (Jakarta: Badan Pembinaan Hukum Nasional, (2016)
- Aulia Muthiah, "Tanggung Jawab Pelaku Usaha Kepada Konsumen tentang Keamanan Pangan dalam Perspektif Hukum Perlindungan Konsumen", *Dialogia Iuridica: Jurnal Hukum Bisnis dan Invetasi*, Volume 7, Nomor2, 2016
- Josephine, et all " Perlindungan Konsumen Daring Dan Tanggung Jawab Perusahaan Marketplace Atas Data Privasi Konsumen, *Suara Keadilan*, Vol. 21 No. 1, April 2020, p-ISSN : 1829-684X, e-ISSN : 2621-9174
- Rizal, M.S "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, 10 (2), 2019
- Putu Ari Sara Deviyanti, "Tuntutan Ganti Rugi Penggunaan Data Pribadi Surat Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", Skripsi, Fakultas Hukum Udayana, 2017
- Tia Deja Pohan dan Muhammad Irwan Padli Nasution, " Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce", :

Jurnal Penelitian Bisnis dan Manajemen Vol.1,  
No.3 September 2023

### Internet

<https://www.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel>, diakses pada tanggal 10 Juli 2023

### Undang-Undang

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

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.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Tambahan Lembaran Negara Republik Indonesia Nomor 6820

Peraturan Pemerintah Nomor 71 Tahun 2019, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 6420

Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Berita Negara Republik Indonesia Tahun 2016 Nomor 1829