Padjadjaran Law Review
Volume 9, Nomor 1, 2021

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban *Online Marketplace* dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data

Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, Nafisah Muthmainnah[1]

Abstrak

Berdasarkan data Kementerian Komunikasi dan Informatika, pertumbuhan nilai *e-commerce* di Indonesia menduduki peringkat pertama di dunia dengan persentase sebesar 78%. Pertumbuhan yang pesat ini tentunya akan melahirkan berbagai permasalahan yang tidak dapat dihindari. Salah satu permasalahan yang mencuat ke publik adalah permasalahan kebocoran data pribadi konsumen. Sayangnya, permasalahan tersebut kurang mendapatkan perhatian dari masyarakat yang kemudian menunjukkan bahwa tingkat kesadaran masyarakat terhadap pelindungan data pribadi masih rendah. Pasalnya, masih banyak masyarakat yang secara sukarela memberikan data pribadinya di layanan *online marketplace*, tanpa mengetahui bahwa data tersebut dapat disalahgunakan oleh oknum yang tidak bertanggung jawab sehingga dapat merugikan dirinya sendiri. Penelitian ini mengkaji kebijakan privasi *online marketplace* terkait pelindungan data pribadi dan bentuk pertanggungjawaban *online marketplace* secara preventif maupun represif terhadap kebocoran data. Adapun, penelitian menggunakan jenis penelitian yuridis normatif yang bersumber dari data sekunder meliputi bahan hukum primer berupa peraturan perundang-undangan dan bahan hukum sekunder berupa buku, jurnal, dan referensi yang relevan. Hasil penelitian menunjukkan bahwa kebijakan privasi berbagai *online marketplace* di Indonesia masih belum sesuai dengan peraturan perundang-undangan dan masih belum maksimal dalam melindungi dan menjamin keamanan data pribadi pengguna. Untuk itu, tulisan ini hadir guna meningkatkan kesadaran pihak-pihak terkait meliputi 1) pemerintah untuk segera mengesahkan Rancangan Undang-Undang Pelindungan Data Pribadi; 2) penyedia layanan *online marketplace system* untuk meningkatkan kualitas pelindungan data pribadi konsumen; 3) masyarakat untuk meningkatkan kesadaran akan pentingnya pelindungan data pribadi di era revolusi industri.
Kata kunci: *e-commerce*, kebocoran data, *online marketplace*, pelindungan data pribadi

Legal Analysis of Online Marketplace Privacy Policy and Accountability in Protection of Users' Personal Data on Data Leakage Cases

Abstract

Following data from the Ministry of Communication and Informatics, Indonesia ranked first as the highest country with e-commerce growth's value in the world is up to 78%. This rapid growth will indubitably give rise to various problems that unavoidable. One of the problems that have risen to the public is data leakage. Unfortunately, data breaches were lack of recognition by the public. It showed the level of public awareness of personal data protection is still low. The reason is, there are still many people who voluntarily provide their personal data in-services online marketplace, without knowing that this data can be misused by irresponsible people so that it can harm themselves. This study examines the privacy policies of online marketplace related to personal data protection and forms of online marketplace preventive and repressive for data leakage. In addition, this research applied a normative juridical approach to the secondary data. Whereas, including primary legal materials in the form of statutory regulations, and secondary legal materials such as books, journals, and relevant references. This research results that privacy policies of various online marketplaces in Indonesia disobeyed the laws and regulations and are still not optimal in protecting and ensuring the security of users' data. Hence, this paper aims to raise awareness of related parties: 1) the government to immediately ratify the Personal Data Protection Bill; ***2)*** *in-service provider online marketplace system to improve the quality of consumer personal data protection; 3) the public to raise awareness of data protection in the era of the industrial revolution.*
Keywords: e-commerce, data leakage, online marketplace, personal data protection

[1] Fakultas Hukum Universitas Padjadjaran, Fakultas Hukum, Kampus Unpad Jatinangor, Jl. Raya Bandung-Sumedang Km. 21 Jatinangor, Kab. Sumedang 45363 Jawa Barat, maichle19001@mail.unpad.ac.id, farah18011@mail.unpad.ac.id, farah18011@mail.unpad.ac.id, farah18011@mail.unpad.ac.id

P-ISSN : 2407-6546
E-ISSN : 2685-2357

A. Pendahuluan

Perkembangan teknologi yang kian masif telah mengubah gaya hidup masyarakat yang semula dilakukan secara tradisional berubah menjadi modern (modernisasi). Modernisasi tentunya berimplikasi ke seluruh aspek kehidupan masyarakat, terutama dalam hal mempermudah akses memperoleh informasi. Kemajuan teknologi yang berkembang pesat mendorong manusia untuk dapat beradaptasi dan berinovasi dalam melakukan kegiatan di berbagai sektor seperti sosial, ekonomi, dan budaya. Dalam perkembangannya, sektor ekonomi menjadi salah satu sektor yang tumbuh secara signifikan. Hal ini dikarenakan lahirnya suatu inovasi perdagangan melalui sistem elektronik atau biasa disebut *e-commerce*, yakni suatu perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik.[2]

Eksistensi *e-commerce* memberikan kemudahan kepada pihak konsumen dalam melakukan transaksi jual beli. Kegiatan bertransaksi yang dulunya harus dilakukan secara tatap muka (konvensional) kini dapat dilakukan melalui ruang virtual (*cyberspace*). Oleh karenanya, konsumen dapat melakukan transaksi jual beli hanya dengan menggunakan internet dimanapun dan kapanpun. Adapun, kegiatan *e-commerce* dapat diselenggarakan melalui berbagai platform yakni *marketplace*, media sosial, dan website. Salah satu platform *e-commerce* yang menjadi tren di tahun 2020 adalah *marketplace*, seperti Tokopedia, Shopee, Bukalapak, Lazada, Bhinneka, dan sebagainya. Selain menjadi tren, *marketplace* juga menjadi platform berbelanja yang paling dipercayai berdasarkan survei yang dilakukan oleh SIRCLO–perusahaan *e-commerce enabler* penyedia solusi bisnis bagi brand–tahun lalu.[3]

Pada tahun 2020, terjadi fenomena melonjaknya kegiatan berbelanja online yang dilakukan oleh masyarakat Indonesia selama wabah pandemi Covid-19.[4] Hal tersebut dikarenakan tuntutan kebutuhan masyarakat yang tidak dapat dipenuhi dengan mobilisasi secara langsung di tengah kebijakan pembatasan yang diberlakukan oleh pemerintah. Berdasarkan data yang dirilis oleh Bank Indonesia pada September 2020, transaksi *e-commerce* di Indonesia meraup nilai transaksi hingga mencapai Rp 180,74 triliun.[5] Nilai transaksi ini menunjukkan bahwa jumlah transaksi *e-commerce* telah meningkat dua kali lipat dari sebelum mewabahnya virus corona. Peningkatan tersebut membuktikan bahwa kemajuan teknologi telah memberikan dampak yang positif terutama dalam sektor ekonomi dan bisnis. Namun, perlu disadari bahwasanya kemajuan teknologi yang pesat tidak hanya memberikan manfaat saja, tetapi juga akan menyulut berbagai permasalahan. Dimana dalam ruang lingkup *e-commerce*, masalah pokok yang sering timbul adalah kebocoran data pribadi. Pada praktiknya, pengguna *online marketplace* diwajibkan untuk

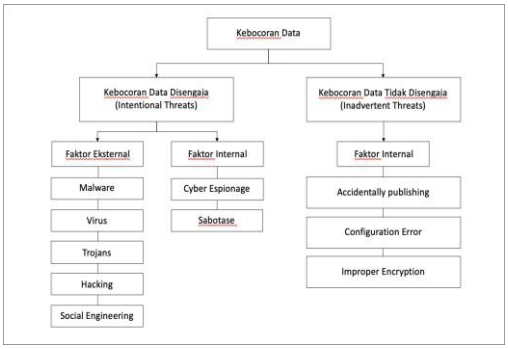
[2] Pasal 1 Angka 24 Undang-Undang 7 Tahun 2014 tentang Perdagangan.

[3] SIRCLO, "Jumlah Pengguna E-Commerce Indonesia di Tahun 2020 Meningkat Pesat", <https://www.sirclo.com/jumlah-pengguna-e-commerce-indonesia-di-tahun-2020-meningkat-pesat/>, diakses pada 13 Mei 2021.

[4] Anam Bhatti (et.al), "E-Commerce Trends During Covid-19 Pandemic", *International Journal of Future Generation Communication and Networking*, Volume 13, Nomor 2, 2020, hlm. 1451.

[5] CNN Indonesia, "Transaksi E-Commerce Capai Rp180,74 T per September 2020", <https://www.cnnindonesia.com/ekonomi/20201215150353-78-582406/transaksi-e-commerce-capai-rp18074-t-per-september-2020>, diakses pada 13 Mei 2021.

mendaftar terlebih dahulu dengan cara mengisi sejumlah data pribadi kepada *platform* tersebut. Dengan diterimanya data pribadi oleh *online marketplace* tersebut memicu kerentanan terjadinya kebocoran data yang akan menimbulkan kerugian bagi para pengguna.



Tabel 1.1. Jenis Kebocoran Data Berdasarkan Penyebabnya

Kebocoran data merupakan sebuah pengungkapan informasi yang bersifat rahasia baik disengaja (*intentional threats*) maupun tidak disengaja (*inadvertent threats*) kepada pihak yang tidak berwenang.[6]

Kebocoran *inadvertent threats* adalah kebocoran data yang bersifat ketidaksengajaan atau kelalaian. Hal ini dapat disebabkan oleh lemahnya sistem keamanan data pribadi konsumen *online marketplace* seperti ketika terjadinya *configuration error* dan *improper encryption* hingga adanya ancaman dari pihak internal seperti *cyber espionage* dan *sabotage* oleh pegawai *online marketplace* untuk membocorkan data-data pribadi tersebut, baik untuk menjualnya kembali atau untuk kebutuhannya sendiri. Selain itu, kebocoran data juga dapat dilakukan secara sengaja yang berasal dari faktor eksternal seperti peretasan data melalui serangan siber misalnya dengan *hacking, virus, trojans*, hingga *encrypting ransomware*.[7]

Kebocoran data pribadi dapat menjadi langkah awal untuk munculnya berbagai macam aktivitas mengganggu seperti *spam* pada *email dan* SMS, dan lain sebagainya. Selain itu, data yang bocor tersebut dapat menimbulkan berbagai kejahatan siber yang merugikan konsumen. Pada praktiknya, seringkali pelaku kejahatan siber melakukan *phishing*, yang merupakan sebuah metode penipuan yang membuat korbannya secara tidak langsung memberikan seluruh informasi yang dibutuhkan oleh sang pelaku.[8] Adapun, metode *phishing* dapat berupa *social engineering attacks*, manipulasi link, hingga *website forgery*.

Kebocoran data pengguna telah terjadi pada beberapa *online marketplace* di Indonesia yakni Tokopedia, Bukalapak dan Bhinneka. Pada tanggal 1 Mei 2020, dilaporkan sebanyak 91 juta data pengguna Tokopedia ditawarkan dalam forum hacker dengan harga US$5.000 sehingga Tokopedia dan KEMENKOMINFO digugat oleh Komunitas Konsumen Indonesia (KKI) senilai Rp 100 miliar.[9] Bocornya data oleh peretas hingga dilakukannya penjualan merupakan indikasi bahwa Tokopedia tidak menjalankan prinsip pelindungan data pribadi dari akses dan pengungkapan yang tidak sah.[10]

[6] Long Cheng (et.al), "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Direction", *WIREs Data Mining and Knowledge Discovery*, 2017, hlm. 1.

[7] *Ibid.*

[8] Mia Haryati Wibowo dan Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime", *Jurnal of Education and Information Communication Technology*, Volume 1, Nomor 1, 2017, hlm. 2.

[9] Zuhri Mahrus, "Kebocoran Data Pengguna Tokopedia, Bukalapak, dan Bhinneka: Siapa Peduli?", <https ://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli>, diakses pada 12 Mei 2021.

[10] Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen", *Proceeding : Call for Paper - 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*,2020, hlm. 51.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Selain Tokopedia, diketahui bahwa sebanyak 13 juta data pengguna Bukalapak diperjualbelikan oleh peretas Pakistan yaitu *Gnostic Players* pada tahun 2019. Berdasarkan rilis resmi dari Bukalapak, dinyatakan bahwa data tersebut diperoleh atas akses tidak sah ke dalam *cold storage backup* di luar sistem Bukalapak. Adapun untuk Bhinneka, data pengguna yang bocor dan ditawarkan dalam *dark web* adalah sebanyak 1,2 juta data.[11] Melalui kasus-kasus di atas, dapat disimpulkan bahwa kebocoran data pengguna telah menjadi suatu ancaman nyata sehingga diharapkan para *online marketplace* di Indonesia dapat meningkatkan upaya preventif dan represif untuk mencegah kebocoran data dan melindungi data pribadi pengguna.

Salah satu bentuk manifestasi pelindungan data pribadi adalah dengan adanya pengaturan yuridis formal yang *sui generis* tentang pelindungan data pribadi. Namun faktanya hingga saat ini Indonesia masih belum memiliki peraturan mengenai pelindungan data pribadi yang terintegrasi dan komprehensif. Kendati demikian, Indonesia sejatinya telah memiliki peraturan yang terpisah secara sektoral mengenai pelindungan data pribadi.[12] Seperti yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Pasal 40 Undang-Undang Nomor 30 Tahun 1999 tentang Telekomunikasi, Pasal 6 Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen PDPSE) dan dalam kaitannya dengan perdagangan melalui sistem elektronik (*e-commerce*) adalah melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Berbagai regulasi yang penulis sebutkan, merupakan bentuk dari perwujudan tanggung jawab negara dalam mengakomodir pelindungan privasi sebagaimana secara tersirat diamanatkan konstitusi melalui Pasal 28 G ayat (1).

Indonesia dapat terbilang cukup tertinggal dalam hal pelindungan data pribadi warga negaranya. Hal ini dapat kita lihat dari perbandingan dengan negara lain seperti Thailand yang telah mengesahkan *Personal Data Protection Act* atau PDPA pada tanggal 28 Mei 2019[13] sebagai payung hukum terhadap pelindungan data pribadi warga negara Thailand. Satu lagi negara tetangga Indonesia yang sudah jauh lebih dahulu mengatur perihal pelindungan data pribadi adalah Malaysia, yang juga merupakan negara pertama yang mempelopori lahirnya regulasi mengenai pelindungan data pribadi di rumpun ASEAN ketika PDPA Malaysia disahkan pada tahun 2013.[14] Permen PDPSE yang dimiliki Indonesia sejatinya belum dapat disetarakan dengan PDPA dari kedua negara tetangga ini disebabkan masih banyak sekali hal-hal yang perlu diatur dalam suatu payung hukum untuk

[11] Zuhri Mahrus, *Op.cit*.
[12] DLA Piper, "Data Protection Laws of The World Thailand vs Indonesia", <https://www.dlapiperdataprotection.com>, diunduh pada 13 Mei 2021.
[13] *Ibid.*
[14] Farah Shahwahid dan Surianam Miskam, "The Personal Data Protection Act 2010: Taking The First Step Towards Compliance", *E-proceedings of the Conference on Management and Muamalah (CoMM 2014)*, 2014, hlm. 154.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

melindungi data pribadi warga negaranya.

Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP) di Indonesia telah melewati berbagai perubahan dari waktu ke waktu sebagai wujud penyempurnaan daripada peraturan yang sudah ada. Tahun 2021 ini, RUU PDP kembali masuk ke dalam Prolegnas Prioritas 2021 dan diharapkan untuk segera disahkan menjadi undang-undang. Dalam perubahan terbaru yang dilakukan pada Januari 2020, Pasal 13 RUU PDP menyebutkan bahwa *"Pemilik Data Pribadi berhak untuk menerima serta menuntut ganti rugi atas pelanggaran Data Pribadinya sesuai dengan ketentuan peraturan perundang-undangan."* dimana nantinya hal ini amat berkenaan dengan pelaksanaan perdagangan dalam sistem elektronik ketika terjadi kasus kebocoran data pemilik data pribadi yang diproses oleh penyelenggara perdagangan dalam sistem elektronik.

Perbedaan tulisan ini dengan penelitian sebelumnya yang ditulis oleh Muhammad Fathur dalam tulisan yang berjudul Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen adalah hasil penelitian ini bukan hanya mengkaji secara umum kelemahan pelindungan data pribadi oleh salah satu *online marketplace* saja, melainkan juga menganalisis secara mendalam berkenaan dengan potensi kebocoran data konsumen dengan memberikan analisis dan komparasi melalui kebijakan privasi yang diterapkan oleh beberapa *online marketplace* dengan hukum positif yang berlaku di Indonesia. Lebih lanjut, perbedaan lainnya terletak pada pertanggungjawaban *online marketplace* pada kasus kebocoran data. Dimana, penelitian ini lebih menekankan tidak hanya terhadap pertanggungjawaban bagi *online marketplace* saja tetapi juga memberikan eksplanasi yang lebih komprehensif terkait kelemahan peraturan perundang-undangan yang mengatur berkaitan dengan pelindungan data pribadi melalui beberapa peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang ITE, PP PSTE, dan Permen PDPSE.

Rumusan Masalah

Dari pemaparan uraian latar belakang tersebut, rumusan masalah yang dijadikan dasar analisis penelitian ini ialah

1. Implementasi pengaturan pelindungan data pribadi dalam kebijakan privasi *online marketplace* berdasarkan hukum positif Indonesia
2. Pertanggungjawaban *online marketplace* dalam pelindungan data pribadi pada kasus kebocoran data.

B. Metode Penelitian

Metode penelitian yang digunakan oleh penulis dalam tulisan ini adalah penelitian secara yuridis-normatif yakni berpedoman kepada norma hukum, prinsip-prinsip hukum, serta hukum positif Indonesia yang memiliki relevansi dengan pelindungan data pribadi (baik yang sudah diundangkan maupun yang belum diundangkan). Penulisan ini mengkaji pokok-pokok permasalahan berkaitan dengan pelindungan data pribadi dengan menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan perbandingan (*comparison approach*). Teknik pengumpulan data utama yang dilakukan penulis adalah dengan studi dokumentasi yang didapat melalui riset secara daring, *focus group discussion* (FGD), dan

P-ISSN : 2407-6546
E-ISSN : 2685-2357

webinar. Selanjutnya, penulis melakukan pengolahan data dengan melakukan kategorisasi, menyusun serta memverifikasi keabsahan dari hasil kolektivitas data tersebut.

Adapun, sumber data yang penulis gunakan dalam penelitian ini adalah data sekunder yang mencakup dua bahan hukum utama yakni bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer merupakan bahan hukum yang bersifat otoritatif yakni meliputi Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Kementerian Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Selain itu, bahan hukum sekunder yakni bahan hukum yang digunakan untuk mendukung bahan hukum primer, yakni terdiri atas Rancangan Undang-Undang Perlindungan Data Pribadi, hasil penelitian terdahulu, buku, jurnal, dan referensi yang memiliki relevansi dengan penelitian ini.

Kemudian, teknik analisis data yang digunakan dalam penelitian ini adalah deskriptif analitik yakni sebuah teknik yang ditujukkan untuk memperoleh visualisasi tentang status gejala yang ada pada saat penelitian (*expose de facto*)[15], sehingga dapat menguraikan secara jelas dan sistematis terhadap pemecahan masalah yang menjadi rumusan masalah utama dalam tulisan ini.

C. Pembahasan dan Analisis

1. Implementasi pengaturan pelindungan data pribadi dalam kebijakan privasi *online marketplace* berdasarkan hukum positif Indonesia

a. Lemahnya kebijakan privasi *online marketplace* dalam memberikan jaminan pelindungan data pribadi

Dalam rangka memberikan jaminan pelindungan data pribadi dalam kegiatan *e-commerce*, seluruh *online marketplace* terikat dalam suatu kewajiban untuk menyediakan sebuah pengaturan kebijakan privasi. Istilah kebijakan privasi dapat dijumpai dalam PP PSTE, yang mendefinisikan bahwa kebijakan privasi merupakan sertifikat keandalan yang jaminan keandalannya adalah memberikan kepastian data pribadi konsumen dilindungi kerahasiaannya sebagaimana mestinya.[16] Selain itu, pengaturan kebijakan privasi dalam *online marketplace* diatur pula dalam UU ITE.[17]

Pada praktiknya, berbagai *online marketplace* telah mematuhi ketentuan tersebut dengan mengintegrasikan kebijakan privasi ke dalam bentuk *e-contract*. Adapun dalam pembahasan ini, penulis akan memaparkan kelemahan dari kebijakan privasi beberapa *online marketplace* di Indonesia, yaitu sebagai berikut:

[15] Winarno Surakhmad, *Penelitian Ilmiah Dasar Metode Teknik*, Bandung: Tarsito, 1990, hlm. 144-146.

[16] Penjelasan Pasal 76 huruf (c), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

[17] Mashitoh Indriyani (et.al), "Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada *Online Marketplace System*", *Justicia Jurnal Hukum*, Volume 1, Nomor 2, 2017, hlm. 196.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

1) Tokopedia[18]

Komitmen nyata Tokopedia dalam menghargai dan melindungi data pribadi pengguna diwujudkan melalui adanya kebijakan privasi. Kebijakan privasi ini menetapkan dasar dalam melakukan segala bentuk pengelolaan data pribadi pengguna baik ketika melakukan pendaftaran, mengakses, atau mempergunakan layanan pada situs. Akan tetapi, terdapat beberapa kebijakan privasi dari Tokopedia yang memiliki kelemahan dan dapat berpotensi mengancam keamanan data serta keselamatan pengguna, antara lain:

a) Perolehan dan Pengumpulan Data Pengguna

Data yang diserahkan secara mandiri kepada pengguna, termasuk namun tidak terbatas pada data yang diserahkan pada saat pengguna mengisi data-data pembayaran pada saat pengguna melakukan aktivitas transaksi pembayaran melalui situs, termasuk namun tidak terbatas pada data rekening bank, kartu kredit, *virtual account, instant payment, internet banking*, dan gerai ritel. Dengan cakupan data pembayaran yang luas dan tidak terbatas tersebut, apabila terjadi kebocoran data maka kemungkinan terburuknya akan mengakibatkan pembobolan terhadap akun bank yang dimiliki pengguna.

Data yang terekam pada saat pengguna mempergunakan situs, termasuk namun tidak terbatas pada data lokasi riil atau perkiraannya seperti alamat IP, lokasi *Wi-Fi*, *geo-location*, dan sebagainya. Ketika terjadi kebocoran, frasa "tidak terbatas" ini dimungkinkan dapat mengancam keamanan dan keselamatan pengguna apabila ternyata data yang diakses adalah sesuatu yang bersifat lebih privasi, terutama ketika data tersebut disalahgunakan.

Selanjutnya, dinyatakan bahwa Tokopedia dapat menggabungkan data yang diperoleh dari sumber tersebut dengan data lain. Faktanya, penggabungan data lain ini tidak dijelaskan secara spesifik berkenaan dengan mekanisme dan jenis data yang digabungkan sehingga dapat memicu lahirnya hasil pengolahan data yang bermasalah. Terlebih lagi, hal ini tidak sejalan dengan Pasal 59 ayat (2) huruf b PP PMSE yang menyatakan bahwa data pribadi harus dimiliki hanya untuk satu tujuan yang telah dideskripsikan secara spesifik serta sah. Data tersebut dilarang untuk diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut.

b) Keamanan, Penyimpanan dan Penghapusan Data Pribadi Pengguna

Dalam ketentuan angka 3, dinyatakan bahwa walaupun Tokopedia telah menggunakan upaya terbaiknya untuk mengamankan dan melindungi data pribadi pengguna, perlu diketahui bahwa pengiriman data melalui internet tidak pernah sepenuhnya aman. Dengan demikian, Tokopedia tidak dapat menjamin 100% keamanan data

[18] Tokopedia, "Kebijakan Privasi", <https://www.tokopedia.com/privacy#keamanan-data>, diakses pada 14 Mei 2021.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

yang disediakan atau dikirimkan kepada Tokopedia oleh pengguna dan pemberian informasi oleh pengguna merupakan risiko yang ditanggung oleh pengguna sendiri. Berdasarkan kebijakan ini, penulis berpandangan bahwa keamanan internet yang rendah tidak dapat dijadikan alasan oleh Tokopedia untuk lepas dari tanggung jawabnya sebagai *online marketplace* yang menyimpan dan menggunakan data pengguna. Selain menjaga dan menjamin data pengguna, Tokopedia wajib meningkatkan *security system,* memeriksa serta memperbaikinya secara berkala.

2) Bukalapak

Kebijakan privasi Bukalapak tunduk terhadap hukum positif Indonesia yang mengatur tentang informasi dan transaksi elektronik, penyelenggara sistem elektronik dan perlindungan data pribadi pengguna serta peraturan pelaksana dan peraturan perubahan yang berhubungan dengan data dan informasi pengguna.[19] Seperti halnya Tokopedia, dalam kebijakan privasi Bukalapak termuat frasa "tidak terbatas" yang salah satunya dapat ditemukan pada kebijakan terkait perolehan dan pelindungan data yang menyatakan bahwa Bukalapak berhak meminta data dan informasi pengguna meliputi perilaku pengguna di Bukalapak dan/atau selama menggunakan layanan informasi pilihan produk, fitur, dan layanan, juga Informasi lain pengguna yang meliputi namun tidak terbatas pada aktivitas pendaftaran, *login*, transaksi, dan lain-lain.[20] Dalam hal ini, Informasi lain yang dikaitkan dengan frasa "tidak terbatas" menjadi sangat samar sehingga pengguna tidak mengetahui sejauh mana data yang diakses dan akibat yang akan timbul kedepannya.

3) Bhinneka

Layaknya *online marketplace* lain, penetapan kebijakan privasi merupakan wujud komitmen dari Bhinneka untuk melindungi dan menghargai data pribadi pengguna. Dinyatakan bahwa, setiap informasi yang pengguna berikan bersifat terbatas untuk tujuan proses yang berhubungan dengan Bhinneka dan tidak untuk tujuan lain. Akan tetapi komitmen tersebut tidak tercermin dalam kebijakan privasi Bhinneka terkait ganti rugi yang menyatakan bahwa Bhinneka tidak bertanggung jawab atas kerugian pengguna yang ditimbulkan oleh tindakan peretasan terhadap data pribadi pada akun pengguna.[21] Kebijakan ini dapat dikatakan sebagai bentuk pelepasan tanggung jawab secara penuh dari Bhinneka sebagai *online marketplace* yang memperoleh, mengumpulkan dan mengolah data pengguna. Terlebih lagi, ketika peretasan oleh pihak ketiga terhadap akun pengguna terjadi maka hal tersebut merupakan bukti bahwa sistem keamanan dari Bhinneka belum memberikan pelindungan. Oleh sebab itu, menurut pandangan penulis, kebijakan ini memperlihatkan bahwa Bhinneka tidak maksimal dalam menjamin keselamatan data pribadi

[19] Bukalapak, "Kebijakan Privasi", <https://www.bukalapak.com/privacy>, diakses pada 14 Mei 2021.

[20] *Ibid*.

[21] Bhinneka, "Kebijakan Privasi", <https://www.bhinneka.com/kebijakan-privasi>, diunduh pada 15 Mei 2021.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

pengguna dengan melepas tanggung jawabnya.

Lemahnya kebijakan *online marketplace* di atas juga diketahui tidak sejalan dengan dua prinsip dalam *Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* yaitu:[22]

1) *Collection Limitation Principle* (Prinsip Pembatasan Pengumpulan)

Prinsip ini menyatakan bahwa harus terdapat batasan dalam pengumpulan data pribadi dan sejenisnya, diperoleh melalui cara yang sah dan adil, serta sesuai dengan persetujuan dari subjek data. Apabila melihat kebijakan privasi ketiga *online marketplace* yang memuat frasa "tidak terbatas" terutama dalam perolehan dan pengumpulan data serta tidak memberikan penjelasan spesifik dalam hal penggabungan data, maka kebijakan tersebut telah tidak sesuai dengan prinsip ini.

2) *Security Safeguards Principle* (Prinsip Perlindungan Keamanan)

Prinsip ini menyatakan bahwa data pribadi harus dilindungi dengan penjagaan keamanan yang wajar terhadap risiko seperti kehilangan atau akses yang tidak sah, perusakan, penggunaan, modifikasi atau pengungkapan data. Kebijakan privasi Tokopedia yang tidak menjamin 100% keamanan data pengguna hingga lepas tangannya Bhinneka terkait pemberian ganti rugi atas tindakan peretasan dapat diketahui tidak memberikan perlindungan dan penjagaan keamanan data pengguna.

b. Legalitas Klausula Baku dalam Kebijakan Privasi *Online Marketplace* ditinjau dari Hukum Positif Indonesia

Sebelum melakukan transaksi dalam *online marketplace*, biasanya pengguna diwajibkan terlebih dahulu untuk menyetujui segala bentuk syarat dan ketentuan maupun kebijakan privasi yang sebelumnya telah dipersiapkan dan ditentukan secara sepihak oleh *online marketplace* yang secara otomatis, hal tersebut menjadi sebuah kontrak baku. Keberadaan kontrak baku tersebut bertujuan untuk memberikan kemudahan bagi para pihak yang terlibat dalam transaksi elektronik. Terlebih dalam transaksi melalui *online marketplace*, persetujuan mengenai persyaratan-persyaratan kontrak baku tersebut dapat tercapai melalui lisensi *click wrap* yang muncul ketika *online marketplace* pertama kali digunakan. Biasanya pengguna ditanya tentang kesediaannya menerima kontrak baku tersebut melalui alternatif "*i accept*" atau "*i don't accept*" sehingga *online marketplace* hanya memerlukan satu atau dua kali klik untuk mendapat persetujuan dari konsumen.[23]

Dengan melakukan klik tersebut, maka pengguna secara otomatis dianggap telah patuh kepada kebijakan privasi maupun syarat dan ketentuan pemakaian aplikasi yang di dalamnya termasuk pemberian akses terhadap data pribadi milik konsumen kepada *online marketplace.* Keabsahan mengenai kontrak elektronik ini

[22] Part Two Number 7 and 11, Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[23] Sinaga, D. H., & Wiryawan, I. W., "Keabsahan Kontrak Elektronik (*e-contract*) Dalam Perjanjian Bisnis", Kertha Semaya: Journal Ilmu Hukum, Volume 8, Nomor 9, 2020, hlm. 1385-1395.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

sendiri diatur dalam UU ITE yang mengatakan bahwa kontrak elektronik merupakan perjanjian para pihak yang dibuat melalui sistem elektronik.

Dalam Pasal 52 PP PMSE disebutkan bahwa kontrak elektronik dikatakan sah serta mengikat apabila kontrak elektronik tersebut telah sesuai dengan syarat serta kondisi dalam penawaran secara elektronik, terdapat kesepakatan di antara pihak yang terlibat, informasi yang tercantum di dalamnya telah sesuai dengan informasi yang tercantum dalam penawaran, dilakukan oleh subjek hukum yang cakap sesuai undang-undang, terdapat hal tertentu, dan objek transaksi dilarang bertentangan dengan peraturan perundang-undangan, ketertiban umum, maupun kesusilaan.

Meski telah memenuhi syarat sahnya perjanjian sebagaimana yang telah dicantumkan dalam KUHPerdata dan PP PMSE, namun sayangnya masih banyak *online marketplace* yang memasukan klausula eksonerasi di berbagai kontrak baku elektronik mengenai kebijakan privasi. Klausula eksonerasi tersebut berupa pengalihan maupun penghapusan tanggung jawab yang seharusnya dibebankan kepada pihak *online marketplace*. Pengalihan tanggung jawab ini contohnya dapat dilihat dari kebijakan privasi Bhinneka yang mengatakan bahwa[24]:

1) Pihak Bhinneka tidak bertanggung jawab atas kebocoran data yang terjadi yang dikarenakan dan/atau terjadi selama Keadaan Memaksa. Dalam hal ini Keadaan Memaksa mencakup namun tidak terbatas pada penutupan, pemogokan, perusahaan, serangan atau ancaman teroris, kebakaran, ledakan, bencana alam atau bencana non alam, pandemi atau epidemi, tidak adanya atau terganggunya jaringan telekomunikasi, informatika, listrik, terjadinya kegagalan sistem yang diakibatkan pihak ketiga di luar kewenangan Bhinneka, terjadinya kegagalan atau tidak berfungsinya sistem dan/atau jaringan perbankan; ketentuan perundang-undangan, peraturan dari pemerintah, putusan pengadilan.
2) Dalam pengaturan mengenai pembatasan tanggung jawab dikatakan bahwa setelah melakukan pemberian informasi data pribadi maka pengguna telah menyetujui bahwa pengguna melepaskan hak atas klaim, kerugian, tuntutan, dan gugatan yang mungkin terjadi atas perolehan, penyimpanan, penggunaan, pemanfaatan, dan/atau pengungkapan informasi data pribadi dalam sistem Bhinneka.
3) Dalam pengaturan mengenai ganti rugi dikatakan bahwa Pengguna setuju untuk Bhinneka (termasuk perusahaan terafiliasi, direktur, komisaris, pejabat, serta seluruh karyawan dan

[24] Bhinneka, "Kebijakan Privasi", <https://www.bhinneka.com/kebijakan-privasi>, diakses pada 15 Mei 2021.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

agen) tidak bertanggung jawab dan pengguna setuju untuk tidak menuntut Bhinneka bertanggung jawab atas segala kerusakan atau kerugian (termasuk namun tidak terbatas pada hilangnya uang, reputasi, keuntungan, atau kerugian tak berwujud lainnya) yang diakibatkan secara langsung atau tidak langsung dari adanya tindakan peretasan yang dilakukan oleh pihak ketiga kepada akun pengguna.

Hal ini menunjukan ketidakmaksimalan peran *online marketplace* sebagai pelaku usaha untuk menjaga data pribadi konsumennya serta menunjukan ketidakpatuhan hukum pelaku usaha terhadap peraturan perundang-undangan. Mengenai klausula baku telah diatur dalam Pasal 18 ayat (1) huruf a Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) yang menyebutkan bahwa dalam menawarkan barang atau jasa untuk diperdagangkan, pelaku usaha dilarang mencantumkan klausula baku pada setiap dokumen maupun perjanjian jika di dalamnya menyatakan pengalihan tanggungjawab oleh pelaku usaha. Ketentuan tersebut kemudian dipertegas dengan Pasal 53 PP PMSE yang menyatakan bahwa klausula baku yang merugikan konsumen seperti yang telah diatur dalam UUPK Pasal 18 merupakan hal yang dilarang dalam kontrak elektronik. Terlebih, kebijakan Bhinneka yang mengatakan bahwa konsumen tidak lagi memiliki hak atas klaim tuntutan, kerugian, hingga gugatan konsumen setelah melakukan pemberian informasi data pribadi atas penyimpanan, perolehan, pemanfaatan, penggunaan, maupun pengungkapan informasi data pribadi yang ada di dalam sistem Bhinneka sangatlah menyalahi aturan serta melanggar hak konstitusional individu.

Apabila terjadi kebocoran data pribadi maupun hal lainnya yang menyebabkan kerugian materil maupun kerugian immaterial dari konsumen, maka hal tersebut dapat dikategorikan juga sebagai perbuatan melawan hukum dikarenakan selain melanggar apa yang tertulis, syarat perbuatan melawan hukum juga termasuk melanggar perbuatan yang tidak sesuai dengan kesusilaan dan kepatutan, ketertiban umum, hingga undang-undang yang berlaku.[25] Dalam hukum perdata sendiri, ganti rugi dapat timbul dikarenakan wanprestasi dan/atau perbuatan melawan hukum.[26] Mengenai hal ini, diatur pula dalam Pasal 18 PP PMSE yang menyatakan bahwa konsumen dapat melaporkan kerugian yang dialami kepada menteri jika perdagangan dilakukan melalui sistem elektronik. Sehingga dapat disimpulkan bahwa hak mengklaim ganti rugi maupun hak gugatan atau tuntutan konsumen tidak dapat dihapuskan.

Online marketplace memiliki kewajiban untuk melindungi data

[25] Lubis, P. P. dan Yunita, Y "Perlindungan Konsumen Terhadap Pencantuman Klausula Eksonerasi Dalam Tiket Bus Antar Kota Antar Provinsi", *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan*, *Volume 2*, Nomor 1, 2018, hlm. 199-207.

[26] *Ibid.*

P-ISSN : 2407-6546
E-ISSN : 2685-2357

privasi konsumennya dari kemungkinan kebocoran data sebagaimana yang telah dicantumkan dalam Pasal 24 PP PMSE yang mengatakan bahwa *online marketplace* wajib menyediakan pengamanan sistem elektronik yang mencakup prosedur dan sistem pencegahan maupun penanggulangan terhadap ancaman dan juga serangan yang menimbulkan gangguan hingga kerugian. Maka dari itu, *online marketplace* juga tidak boleh sepenuhnya melepas tanggung jawab ketika terjadi peretasan terhadap akun konsumen terutama yang disebabkan oleh ketidakmaksimalan sistem keamanan *online marketplace* tersebut. Pengalihan tanggung jawab tersebut juga melanggar prinsip perlindungan keamanan data (*security safeguards principle*) yang mengharuskan adanya perlindungan data pribadi melalui penjagaan keamanan terhadap risiko seperti perusakan, penggunaan, kehilangan, pengungkapan, hingga modifikasi data yang dilakukan secara tidak sah.[27]

Dalam klausula baku, pelaku usaha berada di posisi yang kuat dikarenakan bebas menentukan isi dari kontraknya serta dapat melepas maupun mengalihkan pertanggungjawabannya dengan adanya klausula eksonerasi. Sedangkan konsumen berada di posisi yang lemah dikarenakan tidak bebas menentukan apa yang diinginkan dalam perjanjian tersebut. Sehingga dapat disimpulkan bahwa klausula eksonerasi ini tentunya sangat merugikan konsumen terlebih dikarenakan kedudukan antara konsumen dan pelaku usaha tidak seimbang.[28]

Akibat hukum dari dicantumkannya klausula eksonerasi dalam sebuah kontrak baku dapat dilihat dalam Pasal 18 UUPK ayat (3) yang menyatakan bahwa klausula baku yang ditetapkan oleh pelaku usaha pada dokumen maupun perjanjian yang memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) dinyatakan batal demi hukum atau dianggap tidak pernah ada.

Bagi *online marketplace* yang melanggar Pasal 62 UUPK *jo.* Pasal 18 UUPK, maka akan dijatuhi denda paling banyak dua milyar rupiah atau pidana penjara paling lama sebanyak lima tahun . Dalam Pasal 63 UUPK dinyatakan bahwa terhadap sanksi pidana tersebut, dapat juga dijatuhkan hukuman tambahan. Contoh hukuman tambahan tersebut adalah perampasan barang, penggantian ganti rugi, pengumuman keputusan hakim, perintah penghentian kegiatan yang menimbulkan kerugian terhadap konsumen, kewajiban penarikan barang dari peredaran hingga pencabutan izin usaha. Hal ini sesuai dengan teori perlindungan data pribadi yakni *interactive justice* yang memungkinkan konsumen mendapatkan

[27] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia", *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, Volume 1, Nomor 1, 2019, hlm. 147-154.

[28] Muhammad Saiful Rizal (et.al), "Perlindungan Hukum atas Data Pribadi bagi Konsumen dalam Klausula Eksonerasi Transportasi Online", *Legality: Jurnal Ilmiah Hukum"*, Volume 27*, Nomor* 1, 2019, hlm. 68-82.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

kompensasi atas kerugian yang ditimbulkan akibat klausula baku dalam kontrak elektronik tersebut. Richard Wright menyebutkan bahwa teori ini menyediakan kompensasi yang merupakan perangkat yang bertujuan untuk melindungi konsumen dari interaksi yang merugikan (*harmful interaction*) yang biasanya diterapkan dalam hukum kontrak, hukum pidana, maupun perbuatan melawan hukum.[29]

2. Pertanggungjawaban *online marketplace* dalam pelindungan data pribadi pada kasus kebocoran data

Secara konseptual, bentuk pertanggungjawaban *online marketplace* sejatinya berpangku pada prinsip praduga untuk selalu bertanggung jawab atau *Presumption of Liability*. Prinsip ini menyatakan bahwa tergugat—dalam hal ini *online marketplace*—dianggap selalu bertanggung jawab sampai ia dapat membuktikan bahwa dirinya tidak bersalah, dan beban pembuktian ada pada tergugat.[30] 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*. Prinsip ini pun telah diadopsi ke dalam regulasi terkait perlindungan konsumen di Indonesia.

Lebih jauh, pertanggungjawaban yang diterapkan dalam kebijakan *online marketplace* terhadap kasus kebocoran data di Indonesia menganut teori *strict liability*. Menurut Sidharta, *strict liability* merupakan wujud distingtif dari suatu perbuatan melawan hukum, yakni prinsip pertanggungjawaban dalam perbuatan melawan hukum 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.[31] Berdasarkan hasil analisis kebijakan privasi *online marketplace* Indonesia di atas, ditegaskan bahwa online market place tidak bertanggungjawab atas kebocoran data yang disebabkan karena suatu keadaan memaksa (force majeure). Hal ini selaras dengan beberapa pendapat ahli yang menafsirkan *strict liability* sebagai suatu tanggung jawab yang menentukan kesalahan tidak sebagai faktor yang pasti, namun terdapat pengecualian yakni suatu *force majeure*.[32] Adapun secara konkret, bentuk pertanggungjawaban *online marketplace* terhadap kasus kebocoran data telah diatur dalam regulasi-regulasi berikut.

a. Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan

[29] Rizki Nurdinisari, "Perlindungan Hukum Terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi dalam Penyelenggaraan Telekomunikasi Khususnya dalam Menerima Informasi Promosi yang Merugikan (*Spamming*)," *Tesis*, Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2013, hlm. 16.

[30] Aulia Muthiah, "Tanggung Jawab Pelaku Usaha Kepada Konsumen Tentang Keamanan Pangan dalam Perspektif Hukum Perlindungan Konsumen", *Dialogia Iuridica: Jurnal Hukum Bisnis dan Investasi*, Volume 7, Nomor 2, 2016, hlm. 9.

[31] Sidharta, *Hukum Perlindungan Konsumen Indonesia*, PT Grasindo, Jakarta, 2000, hlm. 63.

[32] 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 Informasi Dan Transaksi Elektronik", *Skripsi*, Fakultas Hukum Udayana, 2017, hlm. 21-22.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)

Dalam praktiknya jika dilihat dalam kasus kebocoran data salah satu *online marketplace* pada putusan Nomor 235/PDT.G/2020/PN.JkT.PST, salah satu alasan gugatan dalam perkara tersebut adalah pasal 15 ayat (1) UU ITE yang menjelaskan bahwasanya penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik yang handal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Namun, perlu diketahui bahwa pasal 15 ayat (1) tidak akan berlaku apabila penyelenggara sistem elektronik dapat membuktikan adanya keadaan memaksa, dan/atau adanya kesalahan/kelalaian pihak pengguna sistem elektronik.

Pada dasarnya, kelemahan utama yang terdapat didalam UU ITE ini adalah belum secara spesifik mengatur ketentuan pertanggungjawaban *online marketplace* dalam kasus kebocoran data. Termasuk juga, belum diaturnya sanksi atau hukuman secara komprehensif yang dapat dibebankan kepada penyelenggara sistem elektronik, atau dalam konteks ini, *online marketplace*. Penjelasan lebih lanjut diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

b. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

Berdasarkan Pasal 76 PP PSTE, kebijakan privasi termasuk ke dalam salah satu kategorisasi dari sertifikat keandalan. Sertifikat keandalan merupakan sebuah dokumen yang menyatakan bahwa pelaku usaha yang menyelenggarakan transaksi elektronik telah lulus audit atau uji kesesuaian dari Lembaga Sertifikasi Keandalan.[33] Menurut hemat penulis, nomenklatur "pelaku usaha" disini tidak relevan dengan konsep dan praktik yang terdapat di dalam *online marketplace system* sekarang. Dimana secara konseptual *marketplace* disini bukan berperan sebagai pelaku usaha, melainkan berkedudukan sebagai penyedia atau wadah pemasaran produk secara elektronik yang berusaha untuk mempertemukan penjual dengan pembeli untuk dapat saling bertransaksi.[34] Terlebih lagi dalam praktiknya, yang memiliki kewajiban atas pemerolehan sertifikat keandalan tersebut ialah *online marketplace* tersebut, bukan sang pelaku usaha. Oleh karenanya, dibutuhkan penggunaan kata yang relevan sehingga tidak menimbulkan penafsiran ganda yang dapat digunakan sebagai strategi untuk menghindari tanggung jawab yang semestinya.

Selanjutnya, salah satu bentuk pertanggungjawaban *marketplace* pada kasus kebocoran data dapat merujuk kepada pasal 100 ayat (2) PP PSTE

[33] Pasal 1 Angka 27, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

[34] Deni Apriadi dan Arie Yandi Saputra, "E-Commerce Berbasis *Marketplace* Dalam Upaya Mempersingkat Distribusi Penjualan Hasil Pertanian", *Jurnal RESTI*, Volume 1, Nomor 2, 2017, hlm. 132.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

yang menjelaskan mengenai sanksi administrasi, yakni terdiri atas denda administratif, diputuskannya akses, teguran tertulis, penghentian sementara, maupun dikeluarkan dari daftar. Penulis melihat bahwa penerapan sanksi administratif terhadap kasus kebocoran data masih lemah. Hal ini dikarenakan, jika ditinjau secara bebas, dari 104 pasal yang terdapat dalam peraturan tersebut, belum ada satupun ketentuan yang spesifik mengklasifikasikan permasalahan mengenai kebocoran data, sehingga menimbulkan ambiguitas dalam menerapkan sanksi administratif khususnya kepada kasus kebocoran data ini. Namun, setelah penulis kaji secara mendalam, maka penerapan sanksi administrasi dalam kasus kebocoran data paling mendekati kualifikasi pada:

1) Pasal 14 ayat (1) huruf a

"Penyelenggara Sistem Elektronik dalam melakukan pemrosesan Data Pribiadi, wajib melaksanakan prinsip perlindungan Data Pribadi yang meliputi: a. Pengumpulan data pribadi dilakukan dengan cara yang sah secara hukum, adil, terbatas dan spesifik, dan diketahui serta disetujui oleh pemilik data pribadi."

Pada poin a di atas yang berbunyi pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi. Disini penulis menilai frasa "adil" tidak sesuai dengan prinsip kepastian hukum. Hal ini dikarenakan, keadilan itu sendiri merupakan suatu konsep yang abstrak.[35] Dimana, sesuatu yang bersifat abstrak sangat tidak sesuai apabila digunakan dalam sebuah ketentuan hukum. Terlebih lagi, faktanya, konsep keadilan masih menjadi isu yang menjadi perdebatan dalam ilmu hukum sendiri, karena hakikatnya hingga sekarang masih belum ada ukuran pasti yang dapat digunakan untuk menentukan sesuatu itu adil atau tidak.[36]

2) Pasal 14 ayat (5)

"Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik data tersebut jika terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelola,."

Jika ditinjau dengan ketentuan yang sama dalam pasal 40 RUU PDP, penulis menemukan beberapa kelemahan yang sangat fundamental terhadap pengaturan ini. Pertama, waktu pemberitahuan tertulis. Dalam ayat (1) RUU PDP, dijelaskan bahwa maksimal *marketplace* harus memberitahukan secara tertulis kepada pemilik data adalah 3x24 jam, sedangkan dalam pengaturan ini tidak ada. Dengan kata lain, dalam hal apabila terjadi kebocoran data, maka *marketplace* dapat memberitahukan secara tertulis kapan saja, bahkan setelah ada gugatannya. Kedua, subjek pemberitahuan tertulis. Pada ayat (1) RUU PDP dinyatakan bahwa kewajiban *marketplace* untuk memberikan pemberitahuan tertulis bukan hanya ditujukan ke pemilik data

[35] Bahder Johan Nasution, "Kajian Filosofis Tentang Konsep Keadilan Dari Pemikiran Klasik Sampai Pemikiran Modern", *Yustisia*, Volume 3, Nomor 2, 2014, hlm. 123.

[36] *Ibid.*, hlm. 119.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

pribadi saja, melainkan juga kepada Menteri. Dalam hal ini, penulis melihat bahwa dengan adanya pemberitahuan tertulis kepada Menteri, maka dapat meningkatkan usaha represif dalam menanggulangi terjadinya kebocoran data. Ketiga, isi pemberitahuan tertulis. Dalam ayat (2) RUU PDP dijelaskan beberapa format ketentuan penulisan pemberitahuan tertulis yakni terdiri atas data pribadi yang terungkap, kapan dan bagaimana data tersebut terungkap hingga upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi. Disini, penulis menilai pengaturan ini dapat meningkatkan efektivitas dalam menanggulangi kebocoran data terutama dalam memberikan jaminan pelindungan kepada konsumen. Dengan adanya format tersebut, pemilik data pribadi tidak perlu susah payah untuk bertanya lagi dengan informasi yang kurang jelas dan tidak perlu risau jika terjadi kebocoran data, karena dalam pemberitahuan tertulis tersebut sudah dicantumkan upaya untuk penanganan dan pemulihan kebocoran data pribadi tersebut.

c. Peraturan Menteri Kementerian Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permen PDPSE)

Menurut penulis Permen PDPSE merupakan payung hukum yang paling mendekati sesuai untuk diimplementasikan dalam hal pengaturan pelindungan data pribadi konsumen *online marketplace* ketika terjadi indikasi kebocoran data konsumen. Hal ini dikarenakan terdapat beberapa pasal yang telah mengakomodir amanat dari UUD 1945. Salah satunya adalah dalam Pasal 24 ayat (1) RUU PDP yang mengatur perihal informasi yang wajib disampaikan oleh pengendali data pribadi.

Menilai dari klausul yang disebutkan dalam pasal *a quo*, permasalahan yang timbul dari penggunaan nomenklatur yang multitafsir dalam kebijakan privasi suatu *online marketplace* dapat diminimalisir. Karena menurut RUU PDP, dengan adanya klausul jenis dan relevansi data pribadi yang akan diproses serta rincian informasi yang dikumpulkan, membuat *online marketplace* harus memberikan penjelasan yang rinci dan jelas agar dapat dimengerti oleh pemilik data sebelum menyetujui datanya untuk diolah oleh *online marketplace*. Selain itu, Pasal 41 RUU PDP juga mendukung adanya pelindungan secara komprehensif terhadap data pribadi pengguna sebagaimana disebutkan bahwa *"Pengendali Data Pribadi diwajibkan untuk bertanggung jawab atas pemrosesan Data Pribadi serta wajib untuk menunjukkan pertanggungjawabannya dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan Data Pribadi."* Salah satu prinsip pelindungan data pribadi adalah pembatasan pengumpulan[37],

[37] Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Bandung: Refika Aditama, 2015, hlm. 30.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

maknanya adalah harus ada pembatasan yang jelas untuk suatu penyelenggara sistem elektronik ketika mengumpulkan data pribadi penggunanya. Salah satu bentuknya adalah dengan pengumpulan yang sah secara hukum dan adil. Dengan kata lain, *online marketplace* tidak dapat memberikan klausul 'tidak terbatas pada' dalam kebijakan privasi yang mereka buat.

Lebih jelas dalam Permen PDPSE juga disebutkan mengenai kewajiban penyelenggara sistem elektronik terkait dengan kegagalan pelindungan data pribadi penggunanya, dimana hal tersebut tercantum pada Pasal 28 huruf c Permen PDPSE sebagai sebuah upaya preventif. Namun, penulis menilai aspek pelindungan preventif yang diberikan oleh Permen PDPSE masih prematur, mengingat saat ini sudah banyak kejahatan yang berevolusi dalam ranah siber, seperti *ransomware* yang menyerang informasi perusahaan dengan meminta imbalan atas data yang dicuri[38], memasuki *server* suatu perusahaan tanpa izin dengan melewati batas kewenangan atau yang biasa dikenal dengan istilah *hacking*[39], dan *phishing* atau aktivitas seseorang untuk mendapatkan data pribadi pengguna dengan cara menipu korban melalui penggunaan identitas palsu yang menyerupai identitas asli suatu situs resmi. Data pribadi yang dicuri pun amat krusial dan menimbulkan kerugian ekonomi karena informasi yang dicuri *phisher* adalah kata sandi akun atau nomor kartu kredit korban.[40]

Melihat kejahatan yang terus berevolusi, perlu diadakannya suatu upaya preventif yang lebih maksimal berupa payung hukum untuk melindungi data pribadi pengguna agar dapat merasa lebih aman dalam menggunakan *online* bahwa pengendali data pribadi wajib melindungi keamanan data pribadi dengan *marketplace*. Hal ini penulis temukan dalam Pasal 27 RUU PDP yang mengatur melakukan penyusunan dan penerapan langkah teknis operasional dan penentuan tingkat keamanan untuk melindungi data pribadi dari gangguan pemrosesan data. Dimana klausul ini tidak penulis temukan dalam Permen PDPSE. Langkah teknis operasional yang diproposalkan oleh RUU PDP dapat menjadi langkah preventif yang efektif untuk diimplementasikan dalam *online marketplace* dimana nantinya penyelenggara harus memiliki suatu standar operasional prosedur untuk melindungi data pribadi pengguna yang juga merupakan informasi rahasia perusahaan.

Sebagai upaya represif, Permen PDPSE memberikan bentuk pelindungan berupa penyelesaian sengketa yang dilakukan melalui pengaduan kepada Menteri Komunikasi dan Informatika yang dituang dalam Pasal 29 Permen PDPSE. Ayat 3 dalam pasal tersebut

[38] Aini Khalida Muslim (et.al.), "A Study of Ransomware Attacks: Evolution and Prevention", *Journal of Social Transformation and Regional Development* Volume 1, Nomor 1, hlm. 18

[39] Zoran Cekerevac (et. al.), "Hacking, Protection and the Consequences of Hacking", *Komunikacie* Volume 20, Nomor. 2, hlm. 68.

[40] Dian Rachmawati, "Phising sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber", Jurnal Saintikom Volume 13 Nomor 3, hlm. 211

P-ISSN : 2407-6546
E-ISSN : 2685-2357

menjelaskan juga terkait kriteria kegagalan pelindungan kerahasiaan data pribadi apa saja yang dapat menjadi alasan pengaduan, yakni[41]:

a. tidak adanya pemberitahuan yang dilakukan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi oleh Penyelenggara Sistem Elektronik kepada Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lainnya yang mempunyai keterkaitan dengan Data Pribadi tersebut, baik yang berpotensi ataupun yang tidak berpotensi menimbulkan kerugian; atau
b. meskipun telah dilakukan pemberitahuan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi kepada Pemilik Data Pribadi maupun Penyelenggara Sistem Elektronik lainnya yang terkait dengan kegagalan tersebut, namun waktu pemberitahuannya dilakukan terlambat.

Selain itu, Permen PDPSE juga mengatur mengenai sanksi administratif dalam Pasal 36 ayat (1). Dalam pasal tersebut disebutkan bahwa bentuk sanksi dapat berupa peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, dan/atau pengumuman di situs dalam jaringan (*website online*). Kemudian penulis beranggapan bahwa upaya represif yang ditawarkan oleh Permen PDPSE belum dapat mengatur secara efektif peristiwa yang dikhawatirkan terjadi dalam hal kerugian atas bocornya data pribadi. Sementara itu, RUU PDP memberikan jalan keluar lain yakni melalui ketentuan pidana yang diatur dalam Pasal 61 pada ayat (1) yang berbunyi:

(1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan tujuan menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah) atau dengan pidana penjara paling lama 5 (lima) tahun.

Kendati demikian, RUU PDP juga memberikan sanksi administratif dengan klausul yang sama dengan Permen PDPSE. Hanya saja pada Pasal 50 RUU PDP yang mengatur sanksi administratif, dijelaskan secara lebih rinci mengenai pelanggaran pada pasal berapa saja yang akan mendapatkan sanksi administratif. Sanksi pidana yang terdapat dalam RUU PDP tersebut kemudian menjadi suatu *ultimum remedium* sehingga dapat mencapai tujuan hukum yakni keadilan dan kepastian hukum.

D. Penutup

Kesimpulan

Dalam kebijakan privasi beberapa online marketplace, penulis menemukan kejanggalan berupa pencatuman frasa “tidak terbatas”

[41] Pasal 29 Ayat 3 Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

yang tidak sejalan dengan *collection limitation principle* dan ketentuan PP PSTE yang menyebutkan bahwa pemrosesan data pribadi pengguna wajib dilakukan dengan cara yang sah secara hukum, terbatas dan spesifik, adil, dan dengan persetujuan dari pengguna. Selain itu, perlindungan dan penjagaan data pengguna pada kebijakan privasi online marketplace diketahui juga tidak sejalan dengan *security safeguards principle*. Penulis juga menemukan kelemahan berupa pencantuman klausula eksonerasi di dalam kebijakan privasi berbagai *online marketplace*. Adanya klausula tersebut mengidentifikasi adanya ketidaksesuaian kewajiban pelaku usaha untuk melindungi data pribadi konsumennya karena pihak *online marketplace* belum sepenuhnya mematuhi ketentuan klausula baku dalam kontrak elektroniknya seperti apa yang sudah diatur dalam teori pelindungan data pribadi seperti *security safeguards* dan *interactive justice*, UUPK, PP PSTE, dan PP PMSE. Oleh karenanya, penulis menarik kesimpulan bahwa kebijakan privasi berbagai *online marketplace* di Indonesia masih belum sesuai dengan peraturan perundang-undangan dan masih belum maksimal dalam melindungi dan menjamin keamanan data pribadi pengguna.

Sejatinya, pertanggungjawaban *online marketplace* terhadap kasus kebocoran data, mengedepankan prinsip praduga untuk selalu bertanggung jawab dan menganut teori *strict liability*. Lebih lanjut, pertanggungjawaban konkret *online marketplace* dalam hal kebocoran data telah diatur secara implisit dalam beberapa peraturan perundang-undangan di Indonesia secara sektoral yakni melalui UU ITE, PP PSTE, dan Permen PDPSE. Namun, rupanya setelah ditelaah lebih lanjut, substansi peraturan perundang-undangan sebagai payung hukum yang melindungi korban atas kebocoran data pribadi dalam *online marketplace* dianggap belum dewasa dan tidak efisien untuk diimplementasikan. Banyak celah yang dapat diambil oleh *online marketplace* dalam berdalih dan melepas tanggung jawabnya atas kelalaian yang terjadi. Di satu sisi, Indonesia sudah memiliki RUU PDP yang sudah masuk Prolegnas Prioritas yang telah mengatur lebih banyak aspek pelindungan data pribadi baik secara preventif maupun represif.

Saran

Secara preventif, pemerintah harus memberikan pengawasan yang lebih ketat terhadap *online marketplace* yang beroperasi di Indonesia. Pengawasan tersebut dapat berupa pengawasan terhadap keamanan sistem yang digunakan *marketplace* tersebut maupun pengawasan terhadap klausula baku yang tercantum pada kontrak elektronik mengenai kebijakan privasi. Sedangkan secara represif, kebijakan privasi yang mengandung klausula eksonerasi diatur dalam UUPK yang mengatakan bahwa akibatnya adalah batal demi hukum sehingga klausula tersebut harus direvisi. Maka dari itu, o*nline marketplace* yang ada di Indonesia diharapkan mampu menyesuaikan kebijakan privasinya agar sesuai dengan peraturan perundang-undangan yang ada di Indonesia guna menjamin keamanan data pribadi konsumennya dari ancaman kerugian yang terjadi.

Rancangan Undang-Undang Pelindungan Data Pribadi merupakan salah satu upaya terbaik untuk menjadi pertahanan terbaik untuk melindungi data pribadi pengguna *online marketplace*. Dimana dalam RUU PDP, pelindungan diatur secara komprehensif baik secara preventif

maupun represif. RUU PDP yang sudah masuk ke dalam Prolegnas Prioritas (per-2021) diharapkan untuk segera disahkan agar kekosongan hukum mulai terisi, dan kedepannya masyarakat dapat lebih merasa aman dan nyaman ketika menggunakan fitur *online marketplace*.

DAFTAR PUSTAKA

Buku

Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika Aditama, Bandung, 2015.

Sidharta, *Hukum Perlindungan Konsumen Indonesia*, PT Grasindo, Jakarta, 2000.

Winarno Surakhmad, *Penelitian Ilmiah Dasar Metode Teknik*, Tarsito, Bandung, 1990.

Dokumen Lain

Jurnal

Anam Bhatti (et.al), "E-Commerce Trends During Covid-19 Pandemic", International Journal of Future Generation Communication and Networking, Volume 13, Nomor 2, 2020.

Bahder Johan Nasution, "Kajian Filosofis Tentang Konsep Keadilan Dari Pemikiran Klasik Sampai Pemikiran Modern", Yustisia, Volume 3, Nomor 2, 2014.

Cekerevac, Zoran (et.al), "Hacking, Protection and the Consequences of Hacking", Komunikacie Volume 20, Nomor 2, 2018.

Deni Apriadi dan Arie Yandi Saputra, "E-Commerce Berbasis Marketplace Dalam Upaya Mempersingkat Distribusi Penjualan Hasil Pertanian", Jurnal RESTI, Volume 1, Nomor 2, 2017.

Dian Rachmawati, "Phising sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber", Jurnal Saintikom Volume 13 Nomor 3, 2014.

Farah Shahwahid dan Surianam Miskam, "The Personal Data Protection Act 2010: Taking the First Step Towards Compliance", E-proceedings of the Conference on Management and Muamalah, 2014.

Long Cheng (et.al), "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Direction", WIREs Data Mining and Knowledge Discovery, 2017.

Lubis, P. P., dan Yunita, Y "Perlindungan Konsumen Terhadap Pencantuman Klausula Eksonerasi Dalam Tiket Bus Antar Kota Antar Provinsi", Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan, Volume 2, Nomor 1, 2018.

Mashitoh Indriyani (et.al), "Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System", Justicia Jurnal Hukum, Volume 1, Nomor 2, 2017.

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime", Jurnal of Education and Information Communication Technology, Volume 1, Nomor 1, 2017.

Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen", Proceeding: Call for Paper - 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era, 2020.

Aini Khalida Muslim (et.al), "A Study of Ransomware Attacks: Evolution and Prevention", Journal of Social Transformation and Regional Development Volume 1 Nomor 1, 2019.

Aulia Muthiah, "Tanggung Jawab Pelaku Usaha Kepada Konsumen Tentang Keamanan Pangan dalam

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Perspektif Hukum Perlindungan Konsumen", *Dialogia Iuridica: Jurnal Hukum Bisnis dan Investasi*, Volume 7, Nomor 2, 2016.

Muhammad Saiful Rizal (et.al), "Perlindungan Hukum atas Data Pribadi bagi Konsumen dalam Klausula Eksonerasi Transportasi Online", Legality: Jurnal Ilmiah Hukum", Volume 27, Nomor 1, 2019, hlm. 68-82.

Rizki Nurdinisari, "Perlindungan Hukum Terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi dalam Penyelenggaraan Telekomunikasi Khususnya dalam Menerima Informasi Promosi yang Merugikan (Spamming)," Tesis, Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2013, hlm. 16.

Sinaga, D. H., dan Wiryawan, I. W., "Keabsahan Kontrak Elektronik (e-contract) Dalam Perjanjian Bisnis", Kertha Semaya: Journal Ilmu Hukum, Volume 8, Nomor 9, 2020.

Yuniarti, S., "Perlindungan Hukum Data Pribadi Di Indonesia", Business Economic, Communication, and Social Sciences (BECOSS) Journal, Volume 1, Nomor 1, 2019, hlm. 147-154.

Skripsi

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 Informasi Dan Transaksi Elektronik", *Skripsi*, Fakultas Hukum Udayana, 2017.

Tesis

Rizki Nurdinisari, "Perlindungan Hukum Terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi dalam Penyelenggaraan Telekomunikasi Khususnya dalam Menerima Informasi Promosi yang Merugikan (*Spamming*)," *Tesis*, Program Pascasarjana Fakultas Hukum Universitas Indonesia, 2013.

Website

https://www.sirclo.com/jumlah-pengguna-e-commerce-indonesia-di-tahun-2020-meningkat-pesat/

https://www.cnnindonesia.com/ekonomi/20201215150353-78-582406/transaksi-e-commerce-capai-rp18074-t-per-september-2020

https://www.dlapiperdataprotection.com

https ://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli

https://www.sirclo.com/jumlah-pengguna-e-commerce-indonesia-di-tahun-2020-meningkat-pesat/

https://www.cnnindonesia.com/ekonomi/20201215150353-78-582406/transaksi-e-commerce-capai-rp18074-t-per-september-2020

https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli

https://www.dlapiperdataprotection.com

Dokumen Hukum

Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Undang-Undang Republik Indonesia Nomor 7 Tahun 2014 tentang Perdagangan

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Peraturan Menteri Kementerian Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik