



POLICY PAPER

TINJAUAN PENERAPAN REGULASI PERDAGANGAN MELALUI SISTEM ELEKTRONIK (PMSE) DALAM KONTEKS PERLINDUNGAN DATA PRIBADI DAN PERSAINGAN USAHA

**ALSA LC UGM RESEARCH TEAM (ART)
2022/2023**



KATA SAMBUTAN

Assalamualaikum Warahmatullahi Wabarakatuh,
Shalom,
Om Swastiastu,
Namo Buddhaya,
Salam Kebajikan Bagi Kita Semua.

Puji syukur patut kita panjatkan kepada Tuhan Yang Maha Esa karena atas berkat dan karuniaNya *Policy Paper* yang dibentuk oleh ALSA LC UGM *Research Team* dapat selesai dan dirilis secara resmi.

ALSA LC UGM *Research Team* adalah jawaban dari ALSA LC UGM untuk menumbuhkan kekritisn dan kepekaan *member* ALSA LC UGM terhadap isu hukum nasional serta menjadi rekan sekerja masyarakat untuk mencari solusi bagi masalah hukum yang terjadi di masyarakat. ALSA LC UGM *Research Team* dibentuk dari semangat-semangat tersebut yang mana para *researchers* menuangkan kemahirannya dalam membentuk suatu kajian yang holistik. Demi menumbuhkan *member* ALSA LC UGM yang aktif, solutif, dan juga kritis, *researchers* membentuk *policy paper* ini dan juga secara rutin mengadakan diskusi untuk membahas permasalahan hukum ini secara spesifik. Saya berharap, keberadaan *policy paper* ini dapat memberikan suatu penerangan yang lebih dalam isu hukum yang dibahas dan juga dapat menjadi bukti konkrit dari ALSA LC UGM yang aktif, solutif, dan juga kritis.

Saya ucapkan pula, terima kasih kepada seluruh pihak yang turut mensukseskan publikasi *policy paper* ini, mulai dari para mitra bestari, para *researchers*, dan juga *Local Board* ALSA LC UGM periode 2022/2023. Semoga karya ini dapat menjadi tonggak dalam pembaharuan dan pembangunan hukum Indonesia.

Wassalamualaikum Warahmatullahi Wabarakatuh,
Shalom,
Om Shanti Shanti Om,
Namo Buddhaya,
Salam Kebajikan Bagi kita Semua.

*Impact Profound, Together Abound,
ALSA, Always be One!*



Jeremy Andrew Sugih
Director of ALSA LC UGM 2022/2023



MITRA BESTARI



Deswin Nur

Head, Bureau for Public Relations & Cooperation, The Indonesian Competition Commission (KPPU)



Mohammad Reza

Senior Expert of Legal Affairs to KPPU (The Indonesian Competition Commission)



Alfatika Aunuriella Dini

Asst. Professor at Department of Civil Law,
Faculty of Law, Gadjah Mada University



ALSA LC UGM RESEARCH TEAM 2022/2023



Adinda Atmim
Supervising Researcher



Nicholas Aurelius
Leading Researcher



Natasha Fortunita
Leading Researcher



Amanda Rizkya
Leading Researcher



Sarah Dwi Kautsar
Researcher



Eugenia Felicia
Researcher



Arvin Mahiro
Researcher



Muhammad Andhika
Researcher



Afiyah Arinda
Researcher



ALSA LC UGM RESEARCH TEAM 2022/2023



Afita Safanisa
Researcher



Rezaldi Vilentino
Researcher



Dinda Maulidina
Researcher



Rafifah Erma
Researcher

DAFTAR ISI

I. PENDAHULUAN.....	1
A. Latar Belakang.....	1
II. RUMUSAN MASALAH.....	3
III. PEMBAHASAN.....	3
A. Penerapan Regulasi Perlindungan Data Pribadi Dalam PMSE.....	4
1. Kasus Pelanggaran Perlindungan Data Pribadi di E-commerce.....	4
2. Analisis Peraturan mengenai Data Pribadi di Indonesia.....	6
3. Analisis Penerapan Undang-Undang Perlindungan Data Pribadi.....	10
4. Penerapan Penetration Test Dalam Keamanan Perlindungan Data dalam E-Commerce.....	13
B. Penerapan Regulasi Persaingan Usaha dalam PMSE.....	15
1. Analisis Mengenai Algoritme Harga dalam E-Commerce.....	15
2. Analisis mengenai Persaingan Usaha di PMSE.....	17
3. Kegagalan UU Persaingan Usaha dalam Menanggapi Algoritme Harga.....	21
4. Urgensi Perbaikan Pasal 5 UU Persaingan Usaha.....	23
C. Komparasi Regulasi Perlindungan Data Pribadi dan Persaingan Usaha Dalam Sistem Hukum Negara Jepang dan Korea Selatan.....	25
1. Perbandingan de jure Dengan Negara Jepang.....	25
2. Perbandingan de jure Dengan Negara Korea Selatan.....	30
IV. KESIMPULAN DAN REKOMENDASI.....	37
A. Kesimpulan.....	37
B. Rekomendasi.....	38

TINJAUAN PENERAPAN REGULASI PERDAGANGAN MELALUI SISTEM ELEKTRONIK (PMSE) DALAM KONTEKS PERLINDUNGAN DATA PRIBADI DAN PERSAINGAN USAHA

I. PENDAHULUAN

A. Latar Belakang

Pada tahun 2022, Bank Indonesia mencatat bahwa tingginya nilai transaksi perdagangan elektronik atau biasa disebut *e-commerce* di Indonesia telah mencapai angka Rp. 476.500.000.000.000,00 (empat ratus tujuh puluh enam koma lima ratus triliun rupiah).¹ Dapat dijelaskan pula bahwa suatu peningkatan transaksi masyarakat melalui layanan *e-commerce* tidak dapat dilepas dari pembahasan mengenai adanya perkembangan teknologi serta pembangunan infrastruktur yang lebih baik di berbagai daerah di Indonesia.² Selain itu, peningkatan minat masyarakat terhadap pembelian secara *online* melalui *e-commerce* juga dipengaruhi oleh beberapa hal lainnya seperti besarnya promosi, adanya kemudahan dalam pemesanan, serta konsep menghemat waktu dimana masyarakat tidak perlu menuju suatu tempat tertentu untuk membeli sesuatu barang dimana sekarang masyarakat dapat mencari banyak hal secara online.

Dalam transaksi *e-commerce*, umumnya pembeli akan diminta untuk memasukan data-data pribadinya mulai dari pembuatan akun hingga pemesanan dalam laman *website* maupun aplikasi *e-commerce* yang mana data

¹ Novita Intan, "Industri E-Commerce Dorong Transaksi Ekonomi Digital Rp 1.100 Triliun," *Republika Online*, March 9, 2023, <https://ekonomi.republika.co.id/berita/rr8eaw423/industri-e-commerce-dorong-transaksi-ekonomi-digital-rp-1100-triliun>. (diakses pada 12 Oktober 2023)

² Imam Lukito, "Tantangan Hukum Dan Peran Pemerintah Dalam Pembangunan E-Commerce," *Jurnal Ilmiah Kebijakan Hukum* 11, no. 3 (2017): 138, with url "<http://dx.doi.org/10.30641/kebijakan.2017.V11.349-367>".

tersebut akan dikelola oleh perusahaan *e-commerce*.³ Data tersebut nantinya akan dimiliki oleh perusahaan, di mana, di awal pendaftaran akun, pembeli akan diminta persetujuannya agar perusahaan dapat mengakses serta menyimpan data tersebut.⁴ Namun, pembeli tidak dapat memastikan atas bagaimana perusahaan tersebut akan menyimpan maupun menggunakan data pribadi yang telah ia serahkan untuk dapat diproses dan disimpan sebagaimana tercantum di awal pendaftaran. Hal ini pun akan menjadi suatu kerentanan bagi pemilik data pribadi untuk menjaga dan memastikan data pribadinya tidak disalahgunakan oleh perusahaan *e-commerce*.

Selain data pribadi, permasalahan mengenai persaingan usaha kerap ditemukan dalam perdagangan *e-commerce*. Suatu contoh yang dapat diilustrasikan adalah seperti adanya perusahaan-perusahaan besar yang hadir di *e-commerce*. Perusahaan-perusahaan besar ini akan sangat mudah untuk memutar harga penjualan serta memiliki *bargaining power* yang lebih besar dibanding toko-toko kecil seperti *reseller* ataupun toko-toko lainnya sehingga toko-toko kecil yang tidak memiliki.⁵ Selain itu, banyaknya promo-promo maupun adanya skema “jual rugi” yang dapat menghancurkan harga pasar kerap terjadi di perdagangan *online*, yang mana hal ini dapat membawa banyak kerugian turunya harga pendapatan dalam penjualan.⁶

Maka dari itu, hadirilah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (“PP PMSE”) sebagai regulasi yang membahas lebih detail mengenai alur jalannya peraturan dalam

³ Nanami Satyanegara, Joko Priyono, and Darminto Hartono Paulus, “Perlindungan Data Pribadi di Indonesia Dalam Rangka Perdagangan Elektronik (E-Commerce),” *Diponegoro Law Journal* 9, No. 2 (2020), hlm: 431, with url “<https://doi.org/10.14710/dlj.2020.27044>”.

⁴ *Ibid.*

⁵ Direktorat Ekonomi Kedeputan Kajian dan Advokasi Komisi Pengawas Persaingan Usaha. “Ringkasan Eksekutif Penelitian Perilaku Pelaku Usaha di Sektor E-Commerce”. with url “<https://kppu.go.id/wp-content/uploads/2020/07/EkSum-e-commerce-Perilaku-1.pdf>”. (diakses pada 04 Oktober 2023).

⁶ Novina Putri Bestari. “Pengamat Ungkap Pelaku *Predatory Pricing* di *e-commerce*”. CNBC Indonesia. 05 Maret 2021 (diakses 04 Oktober 2023).

lingkup perdagangan *online*. Sebagaimana selama ini belum hadir regulasi yang membahas lebih lanjut mengenai jalannya perdagangan *online* ataupun *e-commerce*, terdapat kekosongan hukum terkait *e-commerce*. Regulasi ini mengatur baik dari permasalahan mengenai perlindungan data pribadi hingga persaingan usaha yang dimungkinkan hadir dalam permasalahan pembelanjaan *e-commerce*. Hadirnya regulasi ini diharapkan dapat memberikan perlindungan hukum serta pengaturan hukum dalam hal-hal yang terjadi terkait perdagangan melalui sistem elektronik (“PMSE”) di Indonesia.

Oleh karena itu, ALSA LC UGM *Research Team* (ART) 2022/2023 menganggap bahwa adanya urgensi dalam pembuatan *policy brief* yang membahas lebih lanjut mengenai bagaimana penerapan regulasi dalam permasalahan perlindungan data pribadi serta persaingan usaha di *e-commerce* Indonesia. *Policy brief* ini hadir untuk meneliti lebih jauh terhadap kedua permasalahan tersebut di *e-commerce* serta hadir memberikan rekomendasi-rekomendasi bagi pemangku kepentingan.

II. RUMUSAN MASALAH

1. Bagaimana penerapan regulasi perlindungan data pribadi dalam Perdagangan Melalui Sistem Elektronik (PMSE)?
2. Bagaimana penerapan regulasi persaingan usaha dalam Perdagangan Melalui Sistem Elektronik (PMSE)?
3. Bagaimana komparasi regulasi perlindungan data pribadi dan persaingan usaha dalam Perdagangan Melalui Sistem Elektronik (PMSE) yang telah diterapkan pada sistem hukum negara Jepang dan Korea Selatan?

III. PEMBAHASAN

Permasalahan yang diangkat oleh kajian ini dapat dibagi menjadi 2 (dua) masalah utama. Pertama, terkait ketentuan perlindungan data pribadi serta keamanan data dalam Perdagangan Melalui Sistem Elektronik (PMSE). Kedua, terkait

permasalahan persaingan usaha yang berlaku dalam Perdagangan Melalui Sistem Elektronik (PMSE). Kajian ini akan membahas masing-masing permasalahan dalam bagian berikut:

A. Penerapan Regulasi Perlindungan Data Pribadi Dalam PMSE

1. Kasus Pelanggaran Perlindungan Data Pribadi di *E-commerce*

Permasalahan keamanan data *e-commerce* kini semakin marak. Kasus kebocoran data telah terjadi di beberapa perusahaan *e-commerce*, salah satunya yang menimpa Bukalapak. Diketahui 13 (tiga belas) juta data pribadi milik pengguna Bukalapak telah dijual oleh akun bernama Asian Boy dan 12 juta lainnya oleh akun bernama Tryhard User⁷ di RaidForums, yaitu forum hacker tempat jual beli database ilegal.⁸ Dalam proses penanganan kasus kebocoran data yang masif ini, nyatanya pihak Bukalapak belum dapat memberikan perlindungan hukum terhadap konsumen yang mengalami kebocoran data. Langkah yang diambil Bukalapak hanya berupa penggantian sistem keamanan data pribadi pengguna sebagai bentuk pencegahan agar tidak terulangnya permasalahan tersebut. Padahal, kebijakan privasi Bukalapak telah disusun sesuai dengan ketentuan hukum yang berlaku di Indonesia yang mengatur tentang informasi dan transaksi elektronik, penyelenggara sistem elektronik, perlindungan data pribadi pengguna, serta peraturan pelaksanaan dan perubahan yang berkaitan dengan data dan informasi pengguna.⁹ Namun, tetap saja kebocoran data tetap terjadi.

⁷Inaz Indra Nugroho, Reza Pratiwi, dan Salsabila Rahma Az Zahro, "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia," *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 1, no. 2 (December 31, 2021): 115–29, with url "<https://doi.org/10.15294/ipmhi.v1i2.53698>".

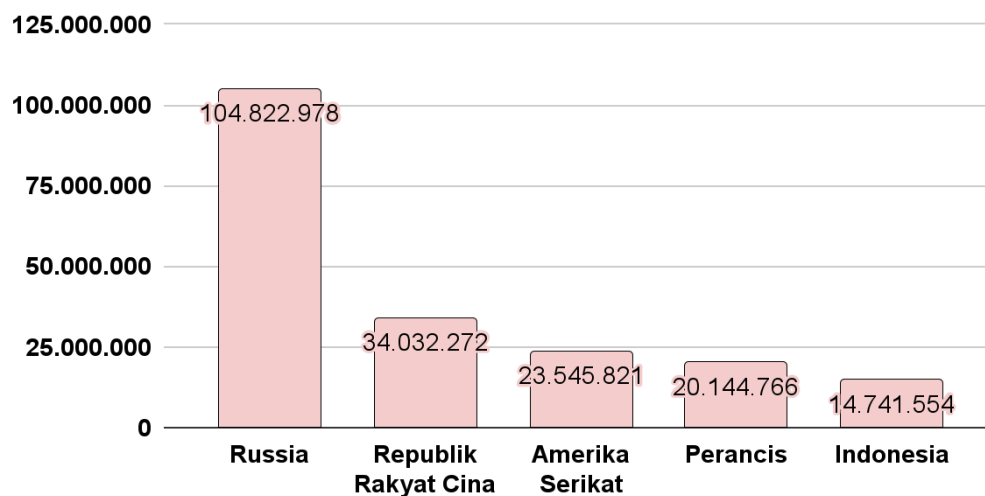
⁸Sean Lyngaas. "FBI and International Partners Seize Control of Popular Hacking Forum". CNN. (12 April 2022).

⁹Maichle Delpiero et al., "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," *Padjadjaran Law Review* 9, No. 1 (August 12, 2021).

Chief Executive Officer (CEO) dari Bukalapak, Rachmat Kaimuddin menjelaskan perusahaan Bukalapak memiliki sistem keamanan yang berlapis dalam menyimpan, menerima, dan mengolah data pengguna. Ketika menerima data, sistem akan menggunakan metode *https* agar data yang masuk tidak akan dicuri. Kemudian, ketika data disimpan, perusahaan Bukalapak menggunakan metode keamanan mutakhir dan berlapis. Dalam pengolahan dan penggunaan data, perusahaan Bukalapak menggunakan pengawasan ketat, sehingga jejak pengakses akan terekam dengan baik.

Pada tahun 2022, Indonesia menduduki posisi 5 besar sebagai negara dengan kasus kebocoran terbesar di dunia.¹⁰

5 Negara Teratas dengan Kasus Kebocoran Data Pada Tahun 2022



**Berdasarkan Data dari Breach Count 2022*

¹⁰ Surfshark, "Data Breach Statistics 2021 vs. 2022," Surfshark, Januari 18, 2023, "<https://surfshark.com/blog/data-breach-recap-2022>".

Melihat seringnya kasus kebocoran data pribadi yang terjadi, hal ini harus menjadi salah satu fokus utama pemerintah Indonesia untuk melindungi hak pribadi masyarakatnya. Kebocoran data pribadi ini disebabkan oleh lemahnya sistem keamanan data yang digunakan oleh pihak *e-commerce* sehingga para peretas dapat dengan mudah masuk dan mencuri data pribadi pengguna *e-commerce* tersebut. Selain itu, kebocoran data pribadi juga dapat disebabkan oleh kurangnya regulasi khusus terkait perlindungan data pribadi yang bersifat lebih mengikat dan kuat.

2. Analisis Peraturan mengenai Data Pribadi di Indonesia

Perlindungan Data Pribadi di Indonesia setidaknya terbagi menjadi 30 undang-undang yang terbagi menjadi kewenangan pada berbagai bidang, seperti telekomunikasi, kesehatan, kependudukan, dan keamanan.¹¹ Oleh karena itu seringkali terjadi tumpang tindih antara bidang-bidang aturan. Faktanya tujuan dari beberapa undang-undang tersebut tetap sama, yaitu perlindungan data pribadi. Perlindungan data pribadi sebenarnya sudah diamanatkan di dalam konstitusi Indonesia, yaitu pada Pasal 28G ayat (1) UUD NRI 1945 “*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*”. Pengertian frasa “Diri Pribadi” dalam Pasal tersebut diperluas maknanya tidak hanya terkait pada diri secara fisik, tetapi

¹¹Nanami Satyanegara, Joko Priyono, dan Darminto Hartono Paulus, “Perlindungan Data Pribadi di Indonesia Dalam Rangka Perdagangan Elektronik (E-Commerce),” *Diponegoro Law Journal* 9, No. 2 (April 2020), with url “<https://doi.org/10.14710/dlj.2020.27044>”.

seluruh informasi berharga terkait pribadi seluruh individu sehingga merupakan hak milik pribadi.¹²

PP PMSE telah disahkan terlebih dahulu sebelum UU Perlindungan Data Pribadi (“UU PDP”). Kendatipun demikian, PP PMSE tetap mengatur mengenai perlindungan data pribadi dalam kegiatan PMSE. Dalam sudut pandang PP PMSE, tujuan dari PP PMSE terkait data pribadi adalah mekanisme penyimpanan data pribadi yang sesuai dengan standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang. Kemudian, ruang lingkup PP PMSE sendiri mencakup hubungan hukum dalam konteks antara pelaku usaha (business to business) maupun pelaku usaha dengan konsumen (*business to customer*).¹³

Berdasarkan Pasal 58 PP PMSE menyebutkan bahwa “*Setiap Pelaku Usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengembal amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan*”. Pasal tersebut menyebutkan bahwa dalam kegiatannya pelaku usaha harus menyimpan data pribadi dari pengguna dengan baik. Kemudian pada Pasal 59 ayat (2) PP PMSE berisi mengenai standar perlindungan data pribadi yang harus dipatuhi oleh pelaku usaha, antara lain (a) data pribadi harus diperoleh secara sah disertai dengan adanya jaminan upaya pengamanan dan untuk mencegah kerugian pemilik data; (b) Tujuan perolehan data pribadi harus dideskripsikan secara spesifik oleh pelaku usaha; (c) Data pribadi yang diperoleh harus relevan dengan tujuan pengolahannya yang sebelumnya sudah disampaikan kepada pemilik data; (d) Data pribadi haruslah akurat dan *up-to-date*; (e) Data pribadi tidak boleh

¹²Maichle Delpiero et al., *Loc Cit.*

¹³*Ibid.*

dikuasai dalam lebih lama dari waktu yang diperlukan dan harus diproses sesuai dengan tujuan perolehan; (f) data pribadi harus diproses sesuai dengan hak subjek pemilik data; (g) Pihak yang menyimpan data harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran data; (h) data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia, kecuali jika negara atau wilayah tersebut dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia. Pasal 58 ayat (3) dan (4) menyebutkan bahwa dalam hal pemilik data pribadi berhenti berlangganan atau menggunakan jasa dan sarana PP PMSE, maka pelaku usaha harus menghapus seluruh data pribadi pemilik data atas permintaan pemilik data pribadi. Terkait dengan Pasal 59 ayat (2) huruf h, Pemerintah nantinya harus mengirimkan daftar *white list countries* sebagai pedoman untuk mengelola data di luar negeri.

Sanksi yang diberikan berdasarkan PP PMSE sendiri hanya terbatas pada sanksi administratif yang diatur pada Bab XVII. Berdasarkan Pasal 80 ayat (2) sanksi administratif tersebut berupa (a) peringatan tertulis; (b) dimasukkan dalam daftar prioritas pengawasan; (c) dimasukkan dalam daftar hitam; (d) pemblokiran sementara layanan PP PMSE; (e) pencabutan izin usaha. Peringatan tertulis diberikan paling banyak 3 (tiga) kali dalam tenggang waktu 2 (dua) minggu terhitung sejak tanggal surat peringatan sebelumnya diterbitkan. Sanksi administratif dalam hal dimasukkan dalam daftar prioritas pengawasan diberikan kepada Pelaku Usaha yang tidak melakukan perbaikan setelah diberikan surat peringatan tertulis ketiga. Frasa daftar hitam yang termaktub dalam Pasal 80 ayat (2) huruf c, maksudnya adalah daftar pelaku usaha yang mempunyai reputasi buruk dan telah terbukti merugikan konsumen, kepentingan nasional, dan/atau keamanan nasional.

Saat ini Indonesia telah mengesahkan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Aturan ini hadir sebagai harmonisasi berbagai macam peraturan mengenai perlindungan data pribadi yang sebelumnya terpecah dalam beberapa bidang. Adapun, UU PDP hadir disahkan setelah PP PMSE. UU PDP membahas secara lebih rinci terkait perlindungan data pribadi termasuk didalamnya berisi sanksi pidana yang mana hal tersebut belum diatur di dalam PP PMSE. Pengaturan mengenai sanksi pidana pokok dalam UU PDP diatur dalam Pasal 67, menurut Pasal 67 ayat (1) menjelaskan bahwa memperoleh atau mengumpulkan data pribadi yang bukan miliknya dan mengakibatkan kerugian Pemilik data pribadi dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Selanjutnya, berdasarkan Pasal 67 ayat (2) menyebutkan, apabila PP PMSE dengan sengaja dan melawan hukum mengungkapkan data pribadi kepada pihak lain diancam pidana penjara paling lama 4 (empat tahun) dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah). Berdasarkan Pasal 67 ayat (3), apabila PP PMSE menggunakan data pribadi yang bukan miliknya secara melawan hukum dan tidak berdasarkan tujuan penggunaan data yang telah disepakati dengan pemilik data pribadi dipidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Selain itu, ketentuan mengenai pidana tambahan diatur dalam Pasal 69 UU PDP berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh (*objectum sceleris*) atau hasil dari tindak pidana (*fructum sceleris*). Selain itu, pada Pasal 70 UU PDP menjelaskan mengenai sanksi pidana yang diberikan kepada subjek Korporasi. Dalam hal tindak pidana yang dimaksud dalam Pasal 67 dan Pasal 68 UU PDP, pengurus, pemegang kendali, pemberi

perintah, pemilik manfaat, dan/atau korporasi dapat diberikan sanksi pidana.¹⁴ Namun, pidana yang dijatuhkan kepada korporasi hanya pidana denda dan pidana tambahan.¹⁵

3. Analisis Penerapan Undang-Undang Perlindungan Data Pribadi

Dalam Pasal 58 PP PMSE, pelaku usaha dapat dianggap sebagai pemilik data pribadi dan wajib bertindak sebagai pengembal amanat data pribadi konsumennya sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Namun, pada kenyataannya, terdapat beberapa pelaku usaha yang gagal dalam menerapkan pasal tersebut, misalnya pada kasus Tokopedia dan Shop Back.¹⁶ Salah satu contohnya, pada Mei 2020, sebanyak 91 juta akun pengguna Tokopedia bocor.¹⁷ Hal ini menunjukkan bahwa sistem pengamanan dan perlindungan data pribadi di Tokopedia masih lemah. Padahal Pasal 59 ayat (2) huruf g PP PMSE mewajibkan pihak yang menyimpan data pribadi untuk memiliki sistem pengamanan yang kuat untuk mencegah terjadinya kebocoran data.

Berangkat dari kasus tersebut, konsumen dapat mengajukan gugatan pertanggungjawaban kepada Tokopedia.¹⁸ Hal tersebut didasarkan pada Pasal 15 ayat 1 dan 2 UU 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pasal 3 ayat (1) Peraturan

¹⁴ *Vide* Pasal 70 ayat (1) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

¹⁵ *Vide* Pasal 70 ayat (2) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

¹⁶ KOMPAS, Conney Stephanie, "7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020". <https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all>. (diakses pada 04 Oktober 2023).

¹⁷ CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual," <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>. (diakses pada 04 Oktober 2023).

¹⁸ Muhammad Fathur, "Tanggung Jawab Tokopedia terhadap Kebocoran Data Pribadi Konsumen," *National Conference on Law Studies: Legal Development towards a Digital Society Era 2, no. 1 (2020)*.

Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan dan Sistem Elektronik, dan Pasal 26 huruf b Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.¹⁹ Namun, dalam mengajukan gugatan, konsumen harus mempertimbangkan biaya, waktu, dan rumitnya proses untuk membuktikan kesalahan Tokopedia. Belum lagi fakta bahwa data yang tersebar tidak akan pernah bisa dihapus. Hambatan tersebut masih kerap berulang bahkan setelah disahkannya UU PDP.

Berdasarkan Pasal 74 UU PDP, 2 (dua) tahun sejak Undang-Undang ini berlakuan terdapat masa transisi, yakni pengendali data pribadi, prosesor data pribadi, dan pihak lain yang terkait dengan pemrosesan data pribadi wajib menyesuaikan dengan Undang-undang ini hingga tahun 2024. Pasca lahirnya UU PDP, kebocoran data masih kerap terjadi, tetapi belum terlihat kebocoran data pribadi pada *e-commerce*.²⁰ Salah satu kasus kebocoran data pribadi yang pernah terjadi pasca lahirnya UU PDP adalah kasus bocornya 300 juta data Dukcapil.²¹ Hal ini menunjukkan bahwa pemerintah masih belum siap untuk menerapkan UU PDP sepenuhnya atau dapat dikatakan bahwa masih dalam proses transisi dan adaptasi, mengingat umur UU PDP baru menjejak usia satu tahun semenjak disahkan menjadi undang-undang.²²

¹⁹ *Ibid.*

²⁰ CNN Indonesia, "Kebocoran Data 300 Juta Data Dukcapil, Pakar Ingatkan Hal Kunci," CNN Indonesia. (2020), with url "<https://www.cnnindonesia.com/teknologi/20230725203819-185-977780/kebocoran-300-juta-data-dukcapil-pakar-ingatkan-3-hal-kunci>". (diakses pada 04 Oktober 2023).

²¹ *Ibid.*

²² CNN Indonesia, "RI sudah punya UU PDP, Kenapa Kebocoran Data Terjadi?," CNN Indonesia. (2023). with url "<https://www.cnnindonesia.com/teknologi/20230717075320-192-974200/ri-sudah-punya-uu-pdp-kenapa-kebocoran-data-masih-terjadi>". (diakses pada 04 Oktober 2023).

Bicara mengenai substansi, UU PDP menyatakan bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga yang akan ditetapkan oleh Presiden.²³ Namun, hingga saat ini belum terdapat keputusan lebih lanjut mengenai penetapan lembaga pengawas Perlindungan Data Pribadi di Indonesia.²⁴ Hal ini menyebabkan adanya kekosongan hukum baik secara normatif maupun praktik. Selain itu, perlindungan data pribadi cenderung diserahkan kepada sebuah lembaga. Bahkan, pada Pasal 49 UU PDP, pengendali data pribadi wajib melaksanakan perintah oleh lembaga. Namun, UU PDP belum menentukan secara gamblang siapa otoritas yang berperan sebagai 'lembaga' ini.²⁵ Oleh karena itu, hingga saat ini, belum terdapat kepastian hukum yang tercermin dari implementasi UU PDP.

Permasalahan lainnya terdapat dalam penerapan sanksi baik secara pidana maupun administrasi dikarenakan interpretasi unsur setiap orang dalam konteks pasal 67 dan 68 UU PDP.²⁶ Interpretasi unsur setiap orang dalam adalah merupakan perorangan atau korporasi.²⁷ Merujuk Pasal 70 UU PDP sanksi pidana terhadap korporasi berupa pidana denda dan pidana tambahan. Pidana denda yang diancam kepada korporasi diancam 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan. Pidana tambahan yang diancam kepada korporasi berupa perampasan keuntungan, pembekuan seluruh atau sebagian usaha korporasi, pelarangan permanen untuk

²³ *Vide* Pasal 52 ayat (2) jo. ayat 3 UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

²⁴ Lely Maulida, "Pengamat: Lembaga Pengawas Independen UU PDP Harus Segera Dibentuk," Kompas, (2022), with url "<https://tekno.kompas.com/read/2022/09/20/17064027/pengamat-lembaga-pengawas-independen-uu-pdp-harus-segera-dibentuk>". (diakses pada 04 Oktober 2023).

²⁵ CNN Indonesia, "UU PDP Berlaku, Kapan Lembaga Pengawas Dibentuk?," CNN Indonesia, (2021), with url "<https://www.google.com/amp/s/www.cnnindonesia.com/teknologi/20221025194729-192-865297/uu-pdp-berlaku-kapan-lembaga-pengawas-dibentuk/amp>", (diakses pada 04 Oktober 2023).

²⁶ *Vide* Pasal 67 dan 68 UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

²⁷ *Vide* Pasal 1 ayat (7) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

melakukan perbuatan, dan pembubaran korporasi.²⁸ Hal ini berimplikasi bahwa adanya perbedaan sanksi yang diberikan terhadap perorangan atau korporasi dengan lembaga di bawah pemerintahan. Implikasinya berupa lembaga pemerintahan tidak dapat dimintakan pertanggungjawaban terhadap kebocoran data pribadi di bawah UU PDP secara pidana. Alternatif satu-satunya yang tersedia adalah sanksi administratif yang dapat diberikan kepada badan publik selaku salah satu subjek yang bisa dianggap sebagai pengendali data pribadi dan prosesor data pribadi.²⁹ Oleh karena itu, terdapat perbedaan pemberian sanksi terhadap perorangan atau korporasi dengan badan publik yang mengakibatkan adanya ketidaktegasan hukum dalam penegakan hukum pelanggaran data pribadi.

4. Penerapan *Penetration Test* Dalam Keamanan Perlindungan Data dalam *E-Commerce*

Definisi mengenai *Penetration Test* adalah metode pengujian yang dilakukan untuk menguji kerentanan sistem dan mengidentifikasi kerentanan keamanan dan konfigurasi, kelemahan perangkat keras dan perangkat lunak, dan kelemahan proses operasional dan penanggulangan teknis.³⁰ Pengujian ini dapat dilakukan secara manual maupun otomatis.³¹ Sebagaimana yang diketahui bahwa *Penetration Test* dilaksanakan untuk menguji jaringan komputer. Dalam konteks *data protection and security*, keamanan jaringan menjadi aspek yang sangat penting demi mencegah terjadi kebocoran data. Apalagi, praktik jual beli yang dilakukan di dalamnya terdapat data-data berharga

²⁸ *Vide* Pasal 70 ayat (4) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

²⁹ *Vide* Pasal 20 ayat (1) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

³⁰ Nugroho Adhi Santoso, Muhamad Ainurohman, dan Rifki Dwi Kurniawan. "Penerapan Metode Penetration Testing Pada Keamanan Jaringan Nirkabel." *Jurnal Responsif: Riset Sains dan Informatika* 4, No. 2 (2022), hlm: 163.

³¹ *Ibid.*

penjual dan pembeli. Tentunya, setiap perusahaan dituntut untuk selalu menjaga kerahasiaan, integritas, dan otentikasi data pada sebuah *Web Server*. Apabila keamanan jaringan tidak diukur dan ditingkatkan secara berkala akan menimbulkan risiko potensi masuknya *hacker* kedalam sistem yang berdampak pada kerusakan atau beralihnya fungsi sistem yang telah dibuat.³² Tidak hanya itu, pada kasus yang paling parah apabila data tersebut diperjualbelikan di suatu *website*.

Sebagaimana yang kita ketahui bahwa keamanan data merupakan aspek yang sangat penting dalam suatu sistem terutama dalam kaitannya dengan tulisan ini, yakni *Data Protection and Security*. *Penetration test* merupakan metode yang mana akarnya berasal dari *ethical hacking*.³³ *Ethical hacking* adalah proses yang berfokus untuk mengamankan dan melindungi data yang rahasia, serta sistem komputer. Prosesnya adalah *hacker* mereview keamanan komputer bukan untuk merusak (*cracker*). Sebaliknya, praktik yang dilakukan adalah menilai keamanan target dan melaporkannya kembali kepada pemiliknya. Pada praktiknya, hal tersebut dilakukan atas dasar izin dari target. Oleh karena itu, tidak boleh jika seseorang dengan serta merta meretas suatu sistem. Pada akhirnya dari kegiatan *ethical hacking* adalah untuk mengisi celah keamanan sistem agar tidak dimanfaatkan oleh pihak-pihak yang merugikan. Dalam hal melakukan *ethical hacking* dikenal 4 (empat) aturan yang tidak boleh dilanggar, yaitu:

1. *Hacker* harus memiliki etika untuk mematuhi aturan yang ditentukan oleh Perusahaan apabila tidak, itu akan membahayakan Perusahaan;

³²Fahmi Fachri, Abdul Fadlil, and Imam Riadi. "Analisis Keamanan Webserver menggunakan *Penetration Test*." *J. Inform* 8, no. 2 (2021), hlm : 183.

³³Shivanshi Sinha and Dr Yojna Arora. "*Ethical Hacking: The Story Of A White Hat Hacker*." *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, ISSN(2020), hlm: 132.

2. *Hacker* harus memiliki itikad baik untuk membantu Perusahaan bukan untuk mengancam atau merugikan Perusahaan;
3. Privasi merupakan hal yang penting dalam *ethical hacking* sehingga seorang *hacker* dalam melakukan *penetration testing* harus menjaga privasi yang telah didapatkan; dan
4. Keterampilan dan kesabaran sangat penting dalam melakukan *penetration testing*.³⁴

Berdasarkan penjelasan diatas, kegiatan tersebut tentunya memicu keuntungan yang dapat dipertimbangkan. Keuntungan yang dimaksud antara lain:³⁵

5. Membantu untuk meminimalisir kebocoran data karena keamanan sistem ditingkatkan secara berkala;
6. Merupakan langkah preventif dari terjadinya kebocoran data;
7. Membantu menemukan celah dan menutup celah sistem tersebut; dan
8. Secara tidak langsung, membantu melawan kejahatan siber.

Penyelenggara PMSE dapat menerapkan *penetration test* agar dapat menjamin keamanan sistem. Pemerintah juga diharapkan dapat mempertegas standar keamanan sistem agar keamanan tersebut dapat ditingkatkan secara berkala.

B. Penerapan Regulasi Persaingan Usaha dalam PMSE

1. Analisis Mengenai *Algoritme Harga dalam E-Commerce*

Digitalisasi bisnis membawa keterbukaan data-data yang dulunya sulit dikumpulkan namun sekarang secara spontan dapat diketahui berbagai pihak. Data seperti statistika pasar dan harga terbuka bagi para pengguna sistem PMSE. Algoritma harga bekerja

³⁴ *Ibid*, hlm:135.

³⁵ Shivanshi Sinha, and Dr Yojna Arora, *op.cit.*, hlm:135.

dengan menganalisis data-data tersebut dan menghasilkan suatu rumusan perhitungan harga yang paling optimal terhadap bisnis dalam kondisi dan waktu tertentu, hal inilah yang disebut *algoritme* harga.³⁶ Penggunaan algoritme harga dalam skala global contohnya seperti perusahaan akomodasi, Airbnb yang mempertimbangkan beberapa hal seperti *review* maupun popularitas.³⁷

Hadirnya penggunaan algoritme dalam PMSE tentu memberikan beberapa dampak positif bagi kemajuan ekonomi digital di Indonesia. Adanya program algoritme dalam PMSE dapat membantu seorang pelaku usaha untuk mengetahui kondisi pasar lebih mendalam melalui *big data*. Akan tetapi, algoritme juga dapat memunculkan disrupsi dalam perkembangan era ekonomi digital. Salah satunya dengan menggunakan sebuah algoritme untuk menetapkan suatu harga terhadap barang dan jasa. Konsep penggunaan algoritme untuk menetapkan harga bukan merupakan suatu hal yang baru. Maskapai penerbangan Amerika Serikat telah menggunakan konsep tersebut sekitar tahun 1980-an, maskapai tersebut menggunakan algoritme harga untuk membantu maskapai mampu bersaing dalam menjual tiket pesawat dengan membuat harga tiket menjadi fluktuatif dan dinamis setelah menyesuaikan keadaan yang pasar yang terjadi pada saat itu³⁸.

³⁶ Julienna Hartono, Julianda Rosyadi, dan Xavier Nugraha. "Analisis Penggunaan algoritme Harga Sebagai Bentuk Perjanjian Penetapan Harga Di Indonesia". *Jurnal Hukum Bisnis Bonum Commune* 4, no. 1. (2021): 38. with url "<https://media.neliti.com/media/publications/458063-none-d0a4920e.pdf>" (diakses pada 04 Oktober 2023)

³⁷ Torsten J. Gerpott dan Jan Berends. "Competitive Pricing on Online Markets: a literature review". *Journal of Revenue and Pricing Management* 21. (2022); 596-622. <https://doi.org/10.1057/s41272-022-00390-x> (diakses pada 04 Oktober 2023).

³⁸ AlgorithmWatch. "Price-fixing algorithms can come, competition authorities are ready, they claim", <https://algorithmwatch.org/en/competition-authorities-ready-for-price-fixing-algorithms/> (diakses pada 30 September 2023).

Namun, terhadap algoritme harga tidak selalu berdampak positif, tetapi menjadi suatu antisipasi jika algoritme harga berdampak negatif. Algoritme harga dapat membawa dampak negatif dikarenakan hal ini dapat melihat pangsa harga pesaing di pasar sehingga menjadikan sebagai salah satu faktor penentuan ataupun pembentuk harga dimana akan munculnya potensi penyalahgunaan algoritme harga untuk menetapkan suatu harga.³⁹ Singkatnya, pelaku pasar mengetahui persis berapa harga yang digunakan oleh kompetitor dan seberapa laku barang dengan harga tersebut dalam pasar. Hal ini dapat mengakibatkan pelaku pasar untuk mengubah harga jualnya sendiri untuk menyesuaikan dengan informasi yang diterima.

2. Analisis mengenai Persaingan Usaha di PMSE

Perdagangan esensinya dilaksanakan dengan landasan prinsip persaingan usaha yang sehat serta pemenuhan hak-hak dan kewajiban pihak yang terlibat. Adapun persaingan usaha sendiri dapat muncul ketika terjadi kondisi dimana terdapat beberapa faktor kesamaan yang dimiliki oleh dua pelaku usaha atau lebih sehingga para pelaku usaha bersaing untuk dapat mengungguli satu sama lain. Faktor kesamaan yang dimaksud dapat berupa kesamaan dalam produk yang dijual dan harga yang ditetapkan. Seiring berkembangnya waktu, iklim persaingan usaha di Indonesia semakin meningkat dengan hadirnya kegiatan dalam *e-commerce*. Persaingan *e-commerce* secara umum dapat dikatakan cukup ketat. Lima *e-commerce* dengan jumlah kunjungan per bulan teratas ialah shopee yang berada di posisi pertama dengan 158 juta kunjungan per bulan, disusul Tokopedia dengan 117 juta kunjungan, di posisi ketiga ada Lazada dengan 83,2 juta

³⁹ Torsten J, Geroitt dan Jan Berends, *loc. cit.*

kunjungan, diikuti oleh Blibli dengan 25,4 juta kunjungan, dan yang terakhir di posisi kelima terdapat Bukalapak dengan 18,1 juta kunjungan⁴⁰.



Data yang telah disajikan menunjukkan bahwa perkembangan *e-commerce* di Indonesia terjadi secara masif. Dengan perkembangan tersebut para pelaku usaha di pasar *e-commerce* juga harus menerapkan strategi usaha yang dapat membantu mereka untuk bersaing di tengah ketatnya persaingan pasar digital. Permasalahan yang kian muncul sebagai akibat dari ketatnya persaingan pasar *e-commerce* adalah penetapan harga tidak wajar, kerjasama antar pesaing dengan tidak wajar dan transaksi merger serta akuisisi⁴¹.

Pengaturan mengenai perdagangan secara umum telah tersusun pada UU Nomor 7 Tahun 2014 tentang Perdagangan. Akan tetapi, dalam UU *a quo* belum terdapat penjelasan secara khusus mengenai

⁴⁰ Adi Ahdiat, "5 *E-commerce* dengan Pengunjung Terbanyak Kuartal I 2023", [databoks.katadata.co.id. https://databoks.katadata.co.id/datapublish/2023/05/03/5-e-commerce-dengan-pengunjung-terbanyak-kuartal-i-2023](https://databoks.katadata.co.id/datapublish/2023/05/03/5-e-commerce-dengan-pengunjung-terbanyak-kuartal-i-2023) (diakses pada September 17, 2023).

⁴¹ Sekolah Tinggi Hukum Indonesia Jember, "Meneropong Persaingan Usaha Sektor E-Commerce di Tengah Pandemi Covid-19", <https://www.jember.ac.id/kabar/meneropong-persaingan-usaha-sektor-e-commerce-di-tengah-pandemi-covid-19> (diakses pada 17 September 2023).

perdagangan elektronik. Oleh karena itu, dalam kaitannya dengan kebutuhan hukum sektor *e-commerce* dikeluarkanlah PP Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE) untuk mengakomodir formil yuridis dari penyelenggaraan kegiatan PMSE. Dalam kaitannya dengan persaingan usaha, dalam PP *a quo* menyatakan bahwa pelaku usaha wajib mematuhi ketentuan peraturan di bidang persaingan usaha⁴². Persaingan usaha diatur dalam Undang-Undang Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat (“**UU Persaingan Usaha**”)

Persaingan usaha pada PMSE juga tunduk kepada hukum pasar pada umumnya. Pada dasarnya, pelaku usaha dalam menetapkan harga akan mempertimbangkan permintaan yang dilakukan oleh konsumen. Menurut teori ekonomi, semakin tinggi harga yang ditetapkan maka permintaan akan berkurang. Begitu pula sebaliknya, permintaan akan meningkat apabila harga yang ditetapkan semakin rendah sehingga dalam menetapkan harga pelaku usaha tidak boleh hanya memperhatikan kepentingannya untuk meraih laba yang diinginkan, tetapi juga harus memperhatikan faktor-faktor lain, seperti persaingan dan ketentuan peraturan perundang-undangan⁴³.

Sebagai salah satu upaya untuk melindungi konsumen terkait penetapan harga, terdapat beberapa kegiatan yang dilarang untuk dilakukan oleh para pelaku usaha, salah satunya adalah dengan menetapkan perjanjian terkait penetapan harga atas barang pada pasar yang sama⁴⁴. Untuk menganalisis pasal *a quo*, terdapat sejumlah pendekatan teoritis sebagai dasar untuk menentukan tindakan yang

⁴² Pasal 26 huruf b PP 80/2019

⁴³ Henri Saragih, “Analisis Strategi Penetapan Harga Dan Pengaruhnya Terhadap Volume Penjualan Pada PT. Nutricia Indonesia Sejahtera Medan,” *Jurnal Ilmiah Methonomi* 1, no. 2 (2015): 46-47

⁴⁴ Pasal 5 ayat (1) UU No.5 Tahun 1999.

perlu diterapkan terhadap pelanggaran UU Persaingan Usaha. Teori pendekatan untuk melakukan pembuktian tersebut dibagi menjadi 2 (dua), yaitu:

1. Teori Pendekatan *Per se Illegal*

Per se Illegal merupakan sebuah pendekatan dimana suatu perjanjian atau kegiatan usaha dilarang karena dampak dari perjanjian tersebut telah dianggap jelas dan pasti mengurangi atau menghilangkan persaingan. Berdasarkan pendekatan tersebut, pelapor tidak perlu membuktikan adanya dampak suatu perjanjian yang dibuat oleh pelaku usaha pesaingnya. Bukti yang diperlukan adalah bahwa perjanjian yang dimaksud telah benar adanya atau bahwa kegiatan bisnis dimaksud telah benar-benar dilakukan oleh pelaku usaha pesaingnya⁴⁵ *Per se Illegal* dapat dikenali pada pasal-pasal yang biasanya menggunakan istilah “dilarang”, tanpa anak kalimat “... yang dapat mengakibatkan...”.

2. Teori Pendekatan *rule of reason*.

Rule of reason merupakan suatu pendekatan yang menentukan meskipun suatu perbuatan telah memenuhi rumusan undang-undang, namun apabila terdapat alasan objektif yang dapat membenarkan perbuatan tersebut, maka perbuatan tersebut bukan merupakan pelanggaran. Artinya penerapan hukumnya tergantung pada akibat yang ditimbulkannya, apakah perbuatan itu telah menimbulkan praktek monopoli atau persaingan usaha tidak sehat, karena

⁴⁵ Ningsih, Ayup Suran. *Implikasi Undang - Undang Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat pada Pelaku Usaha Mikro Kecil dan Menengah (UMKM)*, Jurnal Penelitian Hukum De Jure, Vol. 19 No.2, Juni 2019: hlm 210.

titik beratnya adalah unsur materiil dari perbuatannya⁴⁶. *Rule of reason* dapat diketahui pada undang - undang dari adanya kata “yang dapat mengakibatkan” dan atau “patut diduga”.

Berdasarkan kedua teori pendekatan di atas maka praktik membuat perjanjian dengan pelaku usaha lainnya untuk menetapkan harga akan diberlakukan pembuktian dengan pendekatan *per se illegal*. Hal ini dikarenakan frasa “dilarang” yang kemudian tidak diikuti dengan “... yang dapat mengakibatkan...” dapat ditemukan pada Pasal 5 ayat (1). Meskipun dalam penerapannya, prinsip *per se illegal* dan *rule of reason* ketika dipraktikkan terhadap kasus-kasus persaingan usaha tergantung pada interpretasi hakim. Oleh karenanya, terdapat kemungkinan apabila terdapat kasus yang sama terdapat prinsip yang berbeda⁴⁷ sehingga menjadi penting untuk memperhatikan unsur esensial dalam ketentuan yang berlaku. Elemen esensial yang dapat ditemukan pada pasal *a quo* adalah adanya sebuah perjanjian. Apabila elemen perjanjian dapat ditemukan dalam sebuah kasus maka atas dasar tersebut, pelaku usaha dapat dikenakan sanksi pidana berupa pidana denda atau pidana kurungan pengganti denda menurut ketentuan pada Pasal 48 ayat (2).

3. Kegagalan UU Persaingan Usaha dalam Menanggapi *Algoritme Harga*

Permasalahan timbul lantas ketentuan UU Persaingan Usaha dalam Pasal 5 mewajibkan adanya kesepakatan untuk menentukan penetapan harga. *Algoritme harga* dapat menjadi sebuah tantangan dalam hukum persaingan usaha apabila *algoritme* tersebut diprogram

⁴⁶ *Ibid.*

⁴⁷ Hotana, Melisa Setiawan. *Industri E-Commerce dalam Menciptakan Pasar yang Kompetitif berdasarkan Hukum Persaingan Usaha*. Jurnal Hukum Bisnis Bonum Commune, Vol.1 No.1, Agustus 2018: hlm 33.

secara otomatis untuk menyesuaikan harga dengan kondisi pasar pada saat itu. UU Persaingan Usaha mensyaratkan adanya sebuah perjanjian yang dilakukan oleh pelaku usaha, namun dengan penggunaan algoritme harga, unsur esensial tersebut menjadi hilang dikarenakan algoritme dapat berkoordinasi secara otomatis untuk menyesuaikan harga tanpa perlunya perjanjian yang dilakukan oleh pelaku usaha⁴⁸ sehingga dapat dikatakan sebagai bentuk dari *tacit collusion*. Tantangan lainnya adalah pada proses pembuktian. Sebagaimana yang telah disebutkan sebelumnya, pembuktian dalam penetapan harga dilakukan dengan pendekatan *Per se Illegal* maka dalam hal ini harus ditemukan adanya perjanjian yang dilakukan para pelaku usaha. Namun dalam *tacit collusion* yang menggunakan algoritme pembuktian sulit dilakukan karena sulit terdeteksi. Selain itu, program algoritme seperti ini memungkinkan tidak adanya intervensi dari pelaku usaha karena bersifat otomatis.⁴⁹

Terbatasnya pengaturan terkait dengan *big data* dalam persaingan usaha di Indonesia menjadi hal yang harus diperhatikan. Sebab efek dari penetapan harga menggunakan algoritme dapat merugikan konsumen apabila harga yang ada pada pasaran terus mengalami kenaikan secara drastis. Konsumen akan mengalami kesulitan untuk menyesuaikan dan beradaptasi dengan harga pasar yang dapat mengakibatkan menurunnya permintaan terhadap barang dan jasa. Hal ini juga dapat berdampak buruk bagi perekonomian di Indonesia. Hingga saat ini pun masih belum ada peraturan yang mengatur mengenai permasalahan *tacit collusion* dengan penggunaan

⁴⁸ Cassey Lee, "Competition Policy in the Age of Algorithms: Challenges for Indonesia," *Bulletin of Indonesian Economic Studies* 58, no.3, (2022): 304, with url "<https://doi.org/10.1080/00074918.2022.2125488>" (diakses 10 Oktober 2023).

⁴⁹ Sheng Li, Claire Chunying Xie, Emilie Feyler, "Algorithms & Antitrust: an overview of EU and national case law", *Concurrences*, October 7, 2021

algoritme. Peraturan yang telah berlaku pun masih belum dapat mengakomodir sisi-sisi persaingan dan lebih berfokus pada perilaku pelaku usaha itu sendiri.⁵⁰

4. Urgensi Perbaikan Pasal 5 UU Persaingan Usaha

Sebagaimana telah dijelaskan diatas, penggunaan dan ketergantungan terhadap penggunaan algoritme harga pasti menjadikan pasar PMSE sensitif terhadap fluktuasi harga pasti menimbulkan dampak negatif terhadap persaingan usaha yang sehat dan dapat merugikan konsumen pasar tersebut.⁵¹ Dalam pertimbangan hukum, telah disinggung bahwa terdapat kekosongan hukum terkait praktik *tacit collusion* yang terjadi bukan karena kesepakatan para pengguna algoritme, namun karena cara kerja sistem tersebut. Lantas, pendekatan hukum mengenai penetapan harga pada UU Persaingan Usaha tidak dapat diaplikasikan.

Elemen yang seharusnya menjadi titik berat KPPU dalam memeriksa algoritme harga bukanlah kesepakatan para pihak, KPPU harus memeriksa bukti tidak langsung yang dapat menerangkan terjadinya *tacit collusion* dan kerugian konsumen pasar. Dikarenakan sifat *tacit collusion* yang tidak memiliki unsur kesepakatan antara pihak, KPPU tidak akan dapat memenuhi unsur kesepakatan dalam rumusan Pasal 5 UU Persaingan Usaha mengenai penetapan harga. Untuk dapat melindungi konsumen daripada *tacit collusion* akibat penggunaan algoritme harga, KPPU harus menerapkan pendekatan *rule of reason* dalam penanganan dugaan penetapan harga dalam PMSE.

⁵⁰ Komisi Pengawas Persaingan Usaha, "Mengulik Persaingan Usaha di Platform Online." kppu.go.id. "<https://kppu.go.id/blog/2021/02/mengulik-persaingan-usaha-di-platform-online/>". (diakses 10 Oktober 2023).

⁵¹ Salcedo, Bruno. "Pricing Algorithms and Tacit Collusion." (2015); 20. with url "<http://brunosalcedo.com/docs/collusion.pdf>". (diakses pada 04 Oktober 2023).

Dalam pembuktian algoritme harga, dikarenakan tidak adanya kesepakatan dalam *tacit collusion*, KPPU tidak dapat menjadikan unsur kesepakatan untuk menentukan apakah tindakan tersebut suatu pelanggaran atau tidak. Nyatanya, meskipun *tacit agreement* bukan suatu hal yang dilarang, hal tersebut berdampak buruk pada persaingan usaha dan dapat merugikan konsumen. Satu-satunya indikator yang dapat dijadikan patokan adalah dampak algoritme harga terhadap pasar⁵².

Bukti tidak langsung, meski sudah digunakan oleh KPPU dalam beberapa perkara⁵³, masih belum diatur secara eksplisit dalam peraturan mengenai persaingan usaha. Padahal pembuktian penggunaan algoritme harga yang merugikan konsumen perlu mengkaji dampaknya terhadap pasar, hal ini berwujud bukti tidak langsung. Model yang dapat dicontoh dalam pembuktian praktek ini adalah analisis distribusi harga pasar. Bukan hanya algoritme, KPPU juga harus bisa mengakses data pasar untuk mengkaji terjadinya kerugian konsumen. Dengan akses data harga pasar, KPPU dapat menilai distribusi harga pelaku usaha, tingkat volitas kenaikan dan penurunan pasar, dan menggunakan perhitungan analisis distribusi untuk menentukan apakah terjadi praktek *tacit collusion* yang mengakibatkan kerugian konsumen⁵⁴.

Tentu saja pembuktian dengan model analisis distribusi harga pasar bukanlah perkara mudah. KPPU memerlukan akses data pasar yang relevan dan kuantitas sampel yang banyak untuk dapat

⁵² William E. Kovacic, M.J. Moltenbrey, dan Nathan Eimer. "The Detection and Punishment of Tacit Collusion". *Loyola Consumer Law Review* 9, No. 2. (1997); 160-164. with url "<http://lawecommons.luc.edu/lclr/vol9/iss2/15>". (diakses pada 04 Oktober 2023).

⁵³ Putusan KPPU Nomor 04/KPPU-I/2016

⁵⁴ Cassey Lee. "Competition Policy in the Age of Algorithms: Challenges for Indonesia". *Bulletin of Indonesian Economic Studies* 58, no.3. (2022); 304-310. <https://doi.org/10.1080/00074918.2022.2125488>. (diakses pada 04 Oktober 2023).

memetakan distribusi dengan tingkat keyakinan probabilitas yang dapat diterima. Belum lagi kompleksitas perhitungan statistika probabilitas yang teramat kompleks, apalagi mengingat jumlah sampel yang banyak. Sejalan dengan pendapat mantan Ketua Komisi Persaingan Usaha tahun 2020 - 2021 Kodrat Wibowo, KPPU harus meningkatkan penelitian serta kemampuannya agar dapat mengkaji algoritme harga dalam PMSE⁵⁵.

C. Komparasi Regulasi Perlindungan Data Pribadi dan Persaingan Usaha Dalam Sistem Hukum Negara Jepang dan Korea Selatan

1. Perbandingan *de jure* Dengan Negara Jepang

a) Ketentuan Perlindungan Data Pribadi Negara Jepang

Perlindungan Data Pribadi di Jepang	
Regulasi	Kerangka utama dalam <i>The Act on the Protection of Personal Information</i> (APPI). Pengaturan lebih lanjut melalui peraturan turunan.
Ketentuan Khusus	<ol style="list-style-type: none"> 1. Pengakuan <i>Special-Care</i> Required Data; 2. Hak Penuh bagi pemilik untuk: menolak memberikan data, memilih bagaimana data diolah, dan meminta penghapusan data pribadi; 3. Teknik pengolahan data anonim; 4. Memiliki lembaga khusus untuk mengawasi (PIPC); dan 5. Ketentuan sanksi dan pidana yang berat.

⁵⁵ Heriani AM. "99.62% Pelaku Usaha Gunakan e-commerce, KPPU Pelajari algoritme Penetapan Harga Perusahaan Digital". *Tribun Kaltim*. (2021). with url"
<https://kaltim.tribunnews.com/2021/03/07/9964-pelaku-usaha-gunakan-e-commerce-kppu-pelajari-algoritme-penerapan-harga-perusahaan-digital>". (diakses pada 04 Oktober 2023).

Implikasi	Pengolahan data memberikan kontrol penuh kepada pemilik data bagaimana data diolah. Pemilik data memegang hak penuh untuk menolak dan meminta data dihapus. Pengawasan dilakukan secara seksama oleh IPCC guna mengantisipasi kebocoran data.
------------------	---

Jepang merupakan salah satu negara pertama di Asia yang mengadopsi regulasi khusus terkait perlindungan data pribadi dalam bentuk *the Act on the Protection of Personal Information* (“APPI”). Namun, setelah terjadi banyak insiden pembobolan data pribadi dan lemahnya upaya hukum terhadap penyelenggara sistem elektronik yang berdomisili di luar negeri, Jepang mengamandemen kembali peraturannya pada tahun 2017 dan 2020.⁵⁶ APPI yang telah diamandemen ini menjadi salah satu peraturan yang mendapatkan *adequacy decision* atau pengakuan dari *European Commission* (“EC”) sebagai negara dengan ketentuan peraturan perundang-undangan terkait perlindungan data pribadi yang memenuhi standar Eropa.⁵⁷

APPI memiliki *extraterritorial reach* yaitu berlaku terhadap semua operator bisnis yang berlokasi di Jepang maupun di luar Jepang, tanpa batas minimal identitas database.⁵⁸ Implikasinya adalah bahwa setiap penyelenggara

⁵⁶ Flora Y. Wang. “Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-JAPAN GDPR Adequacy Agreement”. *Harvard Journal of Law & Technology* 33, no. 2. (2020); 683-690. <https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf> (diakses pada 04 Oktober 2023).

⁵⁷ *European Commission*. “Report from the Commission to the European Parliament and Council on the first review of the functioning of the adequacy decision for Japan {COM(2023) 275 final}”. *Commission Staff Working Paper*. (2023); 1. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=SWD:2023:75:FIN (diakses pada 04 Oktober 2023).

⁵⁸ Atsumi & Sakai. “A Guide to Data Protection in Japan”. (2020); 5-6. with url “<https://www.aplawjapan.com/archives/pdf/data-protection-202009.pdf>”. (diakses pada 04 Oktober 2023).

sistem elektronik, apabila ingin beroperasi di wilayah Jepang, harus taat terhadap ketentuan-ketentuan dalam APPI. Jika ditemukan ketidaksesuaian atau ketidak taatan, maka penyelenggara sistem elektronik tersebut akan tunduk pada ketentuan hukum Jepang dan menerima sanksi dari penetapan pengadilan.

APPI membagi data pribadi menjadi 2 kategori data yang dilindungi, yakni: (1) data personal dan (2) data yang memerlukan perlakuan khusus atau *special care-required data*.⁵⁹ Kategori yang pertama merujuk kepada nama, tanggal lahir, email, data biometrik serta data-data angka yang bisa menunjukkan identitas suatu individual, misal nomor dalam identitas atau paspor. Sementara kategori kedua merujuk kepada data yang bisa menjadi basis diskriminasi seperti riwayat medis, status perkawinan, agama, ras dan lain-lain. Data jenis ini harus diperlakukan secara khusus, tunduk pada lapisan ketentuan perlindungan tambahan, dan memiliki sanksi yang lebih berat jika terjadi pelanggaran. Khusus data jenis kedua, APPI melarang pengumpulan informasi yang memerlukan perlakuan khusus tanpa persetujuan eksplisit pemilik informasi.

Ketentuan-ketentuan dalam APPI jelas menunjukkan bahwa pemegang hak utama atas data pribadi adalah pemiliknya sendiri. Jepang memiliki lembaga *Personal Information Protection Commission* (“**PIPC**”) guna memastikan

⁵⁹ Tomoki Ishiara. “*The Privacy, Data Protection, and Cybersecurity Law Review*”. *The Law Review*. (2022). <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/japan> (diakses pada 04 Oktober 2023).

APPI ditaati oleh pengolah data. Sanksi dan ketentuan pidana dalam APPI juga tergolong cukup berat.

b) Ketentuan Tentang Persaingan Usaha di Jepang

Persaingan Usaha PMSE di Jepang	
Regulasi	Kerangka utama dalam AMA. Pengaturan lebih lanjut melalui peraturan turunan.
Ketentuan Khusus	<ol style="list-style-type: none"> 1. Menitikberatkan kepentingan keadilan dalam penerapan dan penegakan ketentuan persaingan usaha; 2. Mengakui <i>circumstantial evidence</i>; 3. Menggunakan <i>rule of reason</i> dalam pendekatan interpretasi ketentuan persaingan usaha; 4. Diawasi oleh <i>Japan Fair Trade Commission</i> (JFTC); dan 5. Perhatian khusus telah diberikan kepada penggunaan algoritme harga.
Implikasi	Jepang mementingkan perlindungan kepentingan konsumen sebagai fokus utama ketentuan persaingan usaha. Jepang telah memulai ada potensi berbahaya dalam penggunaan algoritme harga. Meski belum ditindak, tetapi JFTC telah memberikan perhatian khusus serta riset terkait hal ini guna mengantisipasi kerugian konsumen imbas algoritme harga,

Ketentuan persaingan usaha Jepang diatur dalam *Japan's Antimonopoly Act* (“AMA”). Secara umum, tujuan inti daripada AMA terletak pada prinsip-prinsip umum persaingan usaha yang sehat dengan menitikberatkan kepentingan keadilan

dalam penerapan dan penegakannya.⁶⁰ Alhasil, pendekatan persaingan usaha di Jepang harus tunduk pada prinsip-prinsip dasar persaingan usaha dan memancarkan unsur keadilan.

Terkait permasalahan persaingan usaha dalam PMSE, Jepang tidak memiliki ketentuan undang-undang khusus mengenai persaingan usaha dalam konteks pasar daring, namun ketentuan AMA tetap berlaku. Terkait algoritme harga, Jepang tergolong negara yang telah mempergunakan algoritme dalam instrumen keuangan pada skala yang masif.⁶¹ Dalam menyikapi algoritme harga, Jepang memiliki permasalahan yang sama yakni munculnya dampak negatif terhadap konsumen daripada *tacit collusion*.⁶² *Japan Fair Trade Commission* (“JFTC”) atau lembaga otoritas dalam persaingan usaha Jepang tetap dapat menerapkan ketentuan AMA dalam menindak praktik ini.

Dalam analisis, terbukti bahwa Jepang mengadopsi model pendekatan *rule of reason* yang memungkinkan JFTC untuk menindak suatu tindakan dengan membuktikan adanya kerugian konsumen akibat tindakan tersebut.⁶³ Dalam konteks algoritme harga, Jepang mengaplikasikan ketentuan AMA dengan menggunakan bukti tidak langsung, yang diakui dalam AMA.⁶⁴ Hal tersebut dilaksanakan dengan melihat apakah

⁶⁰ Toshiaki Takigawa. “Competition Law and Policy of Japan”. *The Antitrust Bulletin* 54, no.3. (2009); 435. <https://doi.org/10.1177/0003603X0905400301> (diakses pada 04 Oktober 2023).

⁶¹ Lawrence White. “Trading: Japan Takes The Lead in Algorithmic Trading”. *Euromoney*. (2010). <https://www.euromoney.com/article/b12khsy5gbkckv/trading-japan-takes-the-lead-in-algorithmic-trading> (diakses pada 04 Oktober 2023).

⁶² Kazuyuki Shimizu. “Pricing Game for Tacit Collusion and Passive Investment”. *Business and Society*. (2023); 323-334. <https://ceur-ws.org/Vol-2348/paper23.pdf> (diakses pada 04 Oktober 2023).

⁶³ Tomonori Maezawa dan Jeffery J. Amato. “Algorithms and AI Under Scrutiny By The Japan Fair Trade Commission”. *Mondaq*. (2021). with url “<https://www.mondaq.com/cartels-monopolies/1062326/algorithms-and-ai-under-scrutiny-by-the-japan-fair-trade-commission>”. (diakses pada 04 Oktober 2023).

⁶⁴ Takashi Yanagawa, Hiroshi Takahashi, dan Shinya Ouchi. *Econo-Legal Studies*. Springer. (2021);71-79.

praktik penggunaan algoritme harga mengakibatkan dampak terhadap pasar dan apakah dampak tersebut merugikan konsumen. Pendekatan *rule of reason*, yang menitikberatkan kepentingan konsumen, memberdayakan JFTC untuk menindak tindakan yang berdampak merugikan konsumen. Hal tersebut menjadi landasan JFTC dalam mengkaji algoritme harga. Kendati demikian, hal tersebut masih tergolong baru dan Jepang masih secara aktif mendalami pendekatan yang sesuai untuk algoritme harga dalam PMSE.

2. Perbandingan *de jure* Dengan Negara Korea Selatan

a) Analisis Peraturan Tentang Perlindungan Data Pribadi di Korea Selatan

Perlindungan Data Pribadi di Korea Selatan	
Regulasi	Kerangka utama dalam <i>Personal Information Protection Act</i> (PIPA). Pengaturan lebih lanjut melalui peraturan turunan.
Ketentuan Khusus	<ol style="list-style-type: none"> 1. Mengatur ketentuan umum dalam PIPA, namun mengatur implementasi dalam peraturan pelaksana 2. Dengan jelas menentukan hak-hak pelaku <i>E-Commerce</i> 3. Memiliki standar teknis keamanan sistem yang harus ditaati oleh penyelenggara PMSE. 4. Diawasi oleh <i>Production Planning and Inventory Control</i> (PIPC).
Implikasi	Dalam PIPA, Korea Selatan telah secara jelas menentukan hak-hak daripada pelaku <i>E-Commerce</i> . Peraturan turunan daripada PIPA juga dengan jelas menetapkan suatu standar keamanan sistem yang harus

	dipenuhi. Korea Selatan juga memiliki lembaga khusus sebagai pengawas perkara persaingan usaha.
--	---

Negeri gingseng, Korea Selatan, merupakan salah satu negara yang berhasil dalam melindungi data pribadi masyarakatnya. Berkaca pada keadaan di Korea Selatan secara empiris, penanganan masalah *cyber* yang sangat rentan terhadap penyerangan data pribadi berhasil ditangani dengan baik.⁶⁵ Hal tersebut diatur dalam *Personal Information Protection Act* (“**PIPA**”) yang disahkan pada 2011.

Dalam dunia E-Commerce, Korea Selatan mengatur dengan baik dan terperinci bagaimana hak dan kewajiban subjek pelaku E-Commerce untuk memastikan data informasi dapat terlindungi. Hal ini disebutkan di dalam Pasal 6 *Korean E-Commerce Act* bahwa “*A business operator shall preserve the records on transactions, such as marks, advertisements and contents of the contracts and execution thereof in connection with electronic commerce transactions and mail orders for a substantial period of time. In such cases, a convenient means of perusal and maintenance shall be provided to consumers.*”⁶⁶ Dimaksudkan bahwa dalam memperoleh penyimpanan data informasi, pelaku usaha wajib menyimpan data transaksi, tanda, iklan dan isi kontrak demi menjaga dan memberikan pelayanan yang nyaman kepada konsumen. Adapun penindakan penyimpangan – penyimpangan dalam menggunakan informasi

⁶⁵ Audrye, Rindu, “Perbandingan Peraturan Mengenai Otoritas Independen pada PDPA 2012 Singapura dan PIPA 2011 Korea Selatan,” with url “<https://heylaw.id/blog/perbandingan-pengaturan-mengenai-otoritas-independen-pada-pdpa-2012-singapura-dan-pipa-2011-korea-selatan>”.(diakses pada 1 September 2023).

⁶⁶ Korean E-commerce Act, *Article 6*.

pribadi sudah diatur dengan baik berdasarkan Peraturan Presiden.⁶⁷

Dalam interpretasi terhadap ketentuan PIPA, dinyatakan bahwa kegiatan yang bersangkutan dengan informasi pribadi di Korea Selatan berada dalam naungan badan independen di bawah Perdana Menteri, yaitu *Personal Information Protection Commission* (“**PIPC**”).⁶⁸ Pengelolaan segala resiko terjadinya penyalahgunaan data, kebocoran, dan faktor lainnya yang dapat merugikan subjek data, menjadi wewenang PIPC untuk memeriksa dan menindak. Oleh karena itu, pengusaha *E-Commerce*, dalam upaya menjaga keamanan konsumen, harus mematuhi peraturan perundang-undangan dan wajib melalui prosedur yang ketat dalam rangka mengumpulkan data yang dapat digunakan untuk keperluan aktivitas di dalam *E-Commerce*. Dalam pengumpulan informasi, terdapat batasan yang wajib untuk dipatuhi yaitu data informasi yang tidak boleh dilakukan pengumpulan. hal ini sudah diatur di dalam Pasal 23 PIPA. Regulasi ini menjelaskan bahwa pihak-pihak yang berwenang atau pihak yang melakukan pengumpulan informasi dilarang mengumpulkan dan/atau menyebarkan informasi seperti Ideologi, kepercayaan, masuk atau keluar dari serikat pekerja atau partai politik, pendapat politik, kesehatan, jenis kelamin, kehidupan, dan informasi pribadi yang mungkin dapat secara nyata mengancam privasi subjek data.⁶⁹

Korean E-Commerce Arc. sebagian besar berisikan tentang perlindungan konsumen. Sehingga, dalam pemanfaatan

⁶⁷ *Ibid.*

⁶⁸ *Personal Information Protection Act.*

⁶⁹ *Ibid.*, Art. 23

data informasi yang bersangkutan dengan konsumen haruslah berdasarkan izin dari konsumen sebagaimana disebutkan di dalam Pasal 16 PIPA.⁷⁰ Oleh karena itu, dalam melindungi hak-hak konsumen, peraturan pelaksana daripada PIPA juga menyebutkan tata cara untuk mengajukan tuntutan jika terdapat kerugian yang dialami akibat penyalahgunaan data informasi pribadi dan kegagalan dari Komisi Perlindungan Informasi Pribadi (KPIP) wajib untuk melakukan ganti kerugian, sampai kepada tahap pemulihan.⁷¹

b) Ketentuan Persaingan Usaha PMSE di Negara Korea Selatan

Persaingan Usaha PMSE di Korea Selatan	
Regulasi	Kerangka utama dalam MRFTA. Pengaturan lebih lanjut melalui peraturan turunan.
Ketentuan Khusus	1. Bertujuan utama untuk menciptakan persaingan yang adil dan bebas; 2. Mengakui <i>circumstantial evidence</i> ; 3. Diawasi oleh <i>Korean Fair Trade Commission</i> (KFTC); dan 4. Ditemukan indikasi kerugian akibat algoritme harga sehingga perhatian khusus telah diberikan kepada penggunaan algoritme harga.
Implikasi	Korea Selatan menginterpretasikan ketentuan persaingan usaha untuk menciptakan persaingan adil dan bebas. Dalam penindakan, penggunaan bukti tidak langsung diakui dan sah. KFTC telah menyadari potensi berbahaya penggunaan

⁷⁰ *Ibid.*, Art. 16

⁷¹ *Ibid.*

	<p>algoritma harga dan telah mulai mendalami hal tersebut, dengan investigasi yang sedang berlangsung terkait potensi perkara perdana penggunaan algoritme harga.</p>
--	---

Persaingan usaha di Korea Selatan diatur di dalam *The Monopoly Regulation and Fair Trade Act* (“MRFTA”) yang menyebutkan bahwa terdapat empat jenis tindakan yang dilarang dilakukan dalam persaingan usaha yaitu *unfair collaborative acts, abuses of dominance, unfair trade practices, mergers and acquisitions that substantially lessen competition in korea*.⁷² Pembentukan MRFTA bertujuan agar terciptanya perdagangan, persaingan adil dan bebas yang mana dapat mendorong terlindunginya konsumen dan mendorong kreativitas wirausaha dalam meningkatkan pembangunan perekonomian nasional.

Pada Bab II MRFTA diatur larangan - larangan yang dilakukan dalam perdagangan pada saat posisi dominan atau dalam posisi monopoli.⁷³ Bahwa pelaku usaha dalam posisi dominan dilarang: (1) untuk melakukan penentuan, pemeliharaan, perubahan harga suatu barang atau jasa secara tidak adil; (2) mengontrol penjualan barang atau penyediaan jasa secara tidak adil; (3) Melakukan campur tangan secara tidak adil terhadap kegiatan usaha badan usaha lain; (4) mengganggu pesaing baru secara tidak adil dalam memasuki pasar; (5) melakukan transaksi yang tidak adil untuk

⁷²Norton Rose, 2021, *Competition Law Fact Sheet*, with url “<https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/competition-law-fact-sheet---korea.pdf?revision=95984c11-776a-4cfa-b174-2c761a5c9975&revision=5249431620867387904>”. (diakses pada 3 September 2023).

⁷³ Bab II MRFTA.

mengecualikan pesaing atau merugikan konsumen secara substansial minat.⁷⁴ Google pernah tergugat atas dugaan pelanggaran atas larangan yang disebutkan dalam pasal ini. Komisi Perdagangan yang Adil Korea menghukum Google dengan denda kurang lebih 180 juta dolar AS, yang mana Google dinyatakan menghalangi produsen smartphone lokal korea untuk melakukan penyesuaian dengan sistem operasi pada Android seperti Samsung.⁷⁵ Hal ini terdapat pada perjanjian anti fragmentasi menjadi penghambat dalam persaingan usaha.

Pada Bab IV tentang Pembatasan Kartel Ilegal, pada intinya, secara umum melarang untuk melakukan tindakan kolaboratif atau perjanjian kerjasama yang tidak adil yang dimaksudkan untuk membatasi persaingan secara tidak wajar.⁷⁶ Hal-hal yang tidak boleh dilakukan oleh kartel diatur dalam pasal 19 MRFTA berupa: (a) Menentukan, mempertahankan, atau mengubah harga; (b) Menetapkan syarat dan ketentuan dalam transaksi barang atau jasa, atau pembayarannya; (c) Pembatasan produksi, distribusi atau transaksi; (d) Membatasi atau mengalokasikan wilayah geografis atau pelanggan; (e) Membatasi pendirian atau perluasan fasilitas dan mencegah pemasangan peralatan baru; (f) Membatasi jenis atau spesifikasi barang atau jasa yang diperdagangkan; (g) Bersama-sama menjalankan bagian pokok suatu usaha atau bersama-sama mendirikan perusahaan dengan tujuan yang sama; (h) menentukan pemenang lelang atau penawaran

⁷⁴ Pasal 3-2 MRFTA.

⁷⁵ *Ibid.*

⁷⁶ Bab IV MRFTA.

tertinggi dalam penawaran atau lelang; (i)Praktik lain apapun yang secara substansial membatasi persaingan di pasar tertentu dengan menghalangi atau mengganggu aktivitas bisnis perusahaan lain.⁷⁷ Dalam penindakannya, KTFC mempergunakan bukti tidak langsung sebagai alat pembuktian tindakan tersebut.

Oleh karena itu, demi dapat ditegakkannya hukum maka dibentuklah *The Fair Trade Commission* (“KTFC”) yang terdapat pada Bab VIII MRFTA. KTFC berada dibawah wewenang Perdana Menteri dan juga berfungsi sebagai badan kuasa yudisial, yang merumuskan dan mengelola kebijakan persaingan dan mempertimbangkan, serta memutuskan dan menangani kasus anti monopoli.⁷⁸ Sehingga, dalam penerapan, pelaku usaha wajib mematuhi peraturan hukum, karena di dalam MRFTA diatur sanksi - sanksi bagi pelaku usaha yang melanggar ketentuan tersebut. Pada permasalahan algoritma harga, KTFC juga telah menempatkan perhatian khusus terhadap algoritma harga dikarenakan adanya indikasi kerugian konsumen.

⁷⁷ *Ibid.*

⁷⁸ Bab VIII MRFTA.

IV. KESIMPULAN DAN REKOMENDASI

A. Kesimpulan

Maka dari itu, dapat ditarik kesimpulan terhadap 2 topik pembahasan di atas. Ketentuan dalam UU PDP bertujuan agar data pribadi, termasuk dalam suatu sistem elektronik, terlindungi dari penggunaan yang tidak diinginkan oleh pemilik data tersebut. Namun sifat PMSE yang sejatinya memerlukan pengumpulan data pribadi para pengguna sistem dan pelaku usaha menyebabkan kerentanan khusus terjadinya kebocoran data pribadi, khususnya mengingat volume besar data pribadi yang disimpan dalam PMSE. Dalam pembahasan, dapat ditarik kesimpulan bahwa adanya regulasi UU PDP terhadap PMSE dianggap masih memerlukan peraturan pelaksana yang lebih teknis untuk mencegah tersebarnya data pribadi dalam PMSE. Terhadap tingginya angka kebocoran data di Indonesia, ALSA LC UGM *Research Team* (ART) 2022/2023 berharap bahwa pihak *e-commerce* dapat berkontribusi dalam menjaga data-data pribadi yang diterima oleh *e-commerce*. Oleh karena itu, ALSA LC UGM *Research Team* (ART) 2022/2023 memberikan rekomendasi berupa adanya penerapan *Penetration Test* guna mendukung keamanan data pribadi yang dimiliki oleh *e-commerce*.

Terhadap ketentuan persaingan usaha, dapat ditarik kesimpulan bahwa pendekatan interpretasi ketentuan persaingan usaha harus bisa mengakomodir digunakannya algoritme harga. Penggunaan alat tersebut, meskipun tidak menyalahi ketentuan dengan mempergunakan keterbukaan harga yang memang tersedia dalam PMSE, memiliki dampak buruk terhadap persaingan usaha yang mungkin dapat mengakibatkan dampak buruk terhadap konsumen dalam pasar. Titik berat pendekatan persaingan usaha haruslah berdasarkan *rule of reason*, yang dapat menindak tindakan yang melukai konsumen pasar.

B. Rekomendasi

Berdasarkan kesimpulan analisis ALSA LC UGM ART 2022/2023, terdapat permasalahan di bidang perlindungan data pribadi dan persaingan usaha dalam PMSE. Kajian ini juga turut mendalami kedua bidang tersebut dengan pendekatan studi komparatif dengan negara Korea Selatan dan Jepang. *Policy Brief* ini dapat memberikan rekomendasi sebagai berikut:

1. Rekomendasi Untuk Permasalahan Perlindungan Data Pribadi Dalam PMSE

- a. Pemerintah
 - i. Segera menetapkan dan membentuk lembaga pengawas perlindungan data pribadi sebagai amanat UU PDP; dan
 - ii. Menerbitkan peraturan pelaksana UU PDP yang pada pokoknya mengatur ketentuan standar teknis pengamanan data dalam PMSE yang harus dipenuhi.
- b. Penyelenggara PMSE
Menyelenggarakan *Penetration Test* terhadap sistem PMSE yang dibuka kepada masyarakat;

2. Rekomendasi Untuk Permasalahan Persaingan Usaha Dalam PMSE

- a. Pemerintah
 - i. Menerapkan pendekatan *rule of reason* dalam ketentuan Pasal 5 UU Persaingan Usaha;
 - ii. Mengakui keabsahan bukti tidak langsung (*circumstantial evidence*) dalam pembuktian perkara persaingan usaha; dan
 - iii. Mengembangkan kemampuan KPPU untuk dalam bidang teknologi informasi dengan menggunakan model analisis distribusi harga sebagai indikator algoritme harga.



UNIVERSITAS
GADJAH MADA



**Impact Profound, Together Abound
ALSA, Always be One!**

**ALSA LC UGM Secretariat
Faculty of Law UGM
Jl. Sosio Yustisia No.1, Bulaksumur
Sleman, D. I. Yogyakarta, 55291**