Jurnal RechtsVinding Media Pembinaan Hukum Nasional ISSN 2089-9009
Volume 12 Nomor 2, Agustus 2023

SERTIFIKAT KEANDALAN PRIVASI SEBAGAI SALAH SATU BENTUK PELINDUNGAN KONSUMEN DI BIDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

(The Privacy Reliability Certificate as One Form of Consumer Protection in The Field of Information and Electronic Transactions)

Adinda Putri Denisa
Fakultas Hukum Universitas Padjadjaran, Kampus Unpad Jatinangor, Ir. Soekarno Km. 21, Jatinangor, Kab. Sumedang.
e-mail: adinda20001@mail.unpad.ac.id

Muhamad Amirulloh
Fakultas Hukum Universitas Padjadjaran, Kampus Unpad Jatinangor, Ir. Soekarno Km. 21, Jatinangor, Kab. Sumedang.
e-mail: muhamad.amirulloh@unpad.ac.id

Helitha Novianty Muchtar
Fakultas Hukum Universitas Padjadjaran, Kampus Unpad Jatinangor, Ir. Soekarno Km. 21, Jatinangor, Kab. Sumedang.
e-mail: helitha.novianty@unpad.ac.id

Abstrak

Penggunaan *e-commerce* di Indonesia mengalami pertumbuhan yang sangat pesat, dimana tidak luput dari permasalahan kebocoran data pribadi konsumen. UU PDP dan PP PMSE telah mewajibkan secara implisit kepada seluruh pelaku usaha *e-commerce* untuk menggunakan Sertifikat Keandalan Privasi sebagai bentuk pencegahan dan penanganan pengaksesan data pribadi secara tidak sah. Sayangnya tidak semua pelaku usaha mematuhi dan memenuhi ketentuan sebagaimana diwajibkan UU PDP dan PP PMSE. Penelitian ini bertujuan untuk mengetahui bagaimana pelaksanaan kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* di Indonesia dan bagaimana pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya kebocoran data pribadi pengguna berdasarkan hukum positif Indonesia. Penelitian ini dilakukan dengan menggunakan metode pendekatan 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 Tokopedia merupakan satu-satunya *platform* yang telah menggunakan Sertifikat Keandalan Privasi ISO/IEC 27701, mengenai kewajiban penggunaan Sertifikat Keandalan serta pertanggungjawaban pelaku usaha atas kebocoran data pribadi sejatinya belum diatur secara eksplisit oleh hukum positif di Indonesia, sehingga perlunya pengaturan secara tegas agar lebih menjamin pelindungan terhadap konsumen.
Kata kunci: Sertifikat Keandalan Privasi, Pelaksanaan, Pertangggungjawaban

Abstract

The use of e-commerce in Indonesia has experienced rapid growth, but it has not been without issues of personal data breaches for consumers. The Personal Data Protection Law (UU PDP) and E-commerce Provider and Electronic System Operator Regulation (PP PMSE) implicitly require all e-commerce businesses to use Privacy Reliability Certificates as a preventive measure and handling unauthorized access to personal data. Unfortunately, not all e-commerce businesses comply with these requirements mandated by the UU PDP and PP PMSE. This research aims to understand how the obligation of using Privacy Reliability Certificates is implemented by e-commerce businesses in Indonesia and how these businesses are held accountable under Indonesian positive law in the event of personal data breaches. The research is conducted using a normative juridical approach, relying on secondary data sources including primary legal materials such as regulations and secondary legal materials like books, journals, news, and relevant references. The research findings show that Tokopedia is the only platform that has implemented the ISO/IEC 27701 Privacy Reliability Certificate. Regarding the obligation of using Privacy Reliability Certificates and the accountability of e-commerce businesses for personal data breaches, there is no explicit regulation under Indonesian positive law. Therefore, there is a need for clear regulations to ensure better consumer protection.
Keywords: *Privacy Reliability Certificate, Implementation, Accountability.*

A. Pendahuluan

Teknologi Informasi dan Komunikasi telah mengubah perilaku manusia secara global dimana menyebabkan perubahan sosial yang signifikan dan cepat.[1] Perkembangan teknologi dan informasi dapat meningkatkan kinerja dan produktivitas, karena memungkinkan melakukan berbagai kegiatan dengan efektif dan efisien, sehingga memudahkan hidup dari yang sebelumnya. Perkembangan teknologi informasi dan komunikasi juga mengakibatkan tidak adanya batas suatu wilayah (*borderless*).[2] Perubahan pesat teknologi informasi kearah kemajuan globalisasi berdampak hampir ke semua aspek kehidupan masyarakat.[3] 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 yang dikenal dengan *e-commerce*, yakni segala kegiatan jual beli atau transaksi yang dilakukan menggunakan sarana media elektronik (internet).[4]

Lahirnya *e-commerce* dalam dunia Informasi dan Transaksi Elektronik sejatinya memberikan kemudahan kepada penjual (*seller*) dan pembeli (*consumer*) dalam melakukan transaksi jual beli. Zaman dahulu, kegiatan transaksi harus dilakukan secara tatap muka (konvensional) atau secara langsung antara penjual (*seller*) dan pembeli (*consumer*), sedangkan kegiatan transaksi pada zaman sekarang dapat dilakukan melalui ruang virtual (*cyberspace*). Oleh karena hal ini, konsumen dapat melakukan transaksi jual beli kapan pun dan dimana pun hanya dengan menggunakan internet. Kegiatan *e-commerce* dapat diselenggarakan melalui beberapa *platform* seperti *marketplace* dan media sosial. *Platform e-commerce* yang menjadi trend pada tahun 2020 hingga saat ini adalah *marketplace* seperti Facebook *Marketplace*, Tokopedia, Bukalapak, Shopee, dan sebagainya.

Sebelum melakukan kegiatan *e-commerce* pada *platform marketplace*, diwajibkan kepada penjual (*seller*) maupun pembeli (*consumer*) untuk mendaftarkan (*registration*) akun terlebih dahulu dengan mengisikan *form* yang telah disediakan oleh *platform marketplace*. *Form* tersebut diisi dengan data pribadi seperti nama lengkap, tanggal lahir, nomor ponsel, email, gender, dan kata sandi.[5] Data pribadi milik penjual (*seller*) maupun pembeli (*consumer*) dikumpulkan oleh *marketplace* untuk diproses. Dalam hal memberikan data pribadi kepada *platform marketplace,* pada dasarnya tidak menjamin sepenuhnya keamanan data pribadi dan privasi, karena justru akan memicu kerentanan terjadinya kebocoran data pribadi yang akan menimbulkan kerugian bagi para pengguna.

Beberapa *platform marketplace* di Indonesia telah terjadi kebocoran data

---

1 Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia* (Bandung: Refika Aditama, 2005), hlm. 1.
2 *Ibid.*
3 OK. Saidin, *Aspek Hukum Hak Kekayaan Intelektual* (Jakarta: Raja Gravindo Persada, 2004), hlm. 519.
4 Sugiharto, "Memanfaatkan E-Commerce Dengan Benar," Kementerian Keuangan, https://www.djkn.kemenkeu.go.id/artikel/baca/15814/Memanfaatkan-E-Commerce-Dengan-Benar.html (diakses 16 Juli 2023).
5 Pusat Bantuan Facebook, "Membuat akun Facebook," Facebook https://id-id.facebook.com/help/188157731232424 (diakses 16 Juli 2023).

pribadi pengguna yaitu Facebook *Marketplace* dan Tokopedia. Pada tahun 2019 terjadi kasus kebocoran data pribadi pada *platform* Facebook termasuk pada Facebook *Marketplace*. Diketahui terdapat data pribadi 553 juta pengguna Facebook bocor dan bisa diakses secara gratis di forum peretas. Pengguna yang datanya bocor tersebar di 106 negara. Negara yang datanya paling banyak bocor adalah Mesir dengan jumlah 44,8 juta pengguna, Tunisia 39,5 juta, Italia 35,6 juta, kemudian Amerika Serikat (AS) 32,3 juta. Sejumlah pengguna Facebook asal Indonesia pun tak luput jadi korban dari kebocoran data ini, dengan jumlah mencapai 130.000 pengguna. Adapun data pribadi yang bocor meliputi informasi nama lengkap, nomor telepon, lokasi, tanggal lahir, ID Facebook, gender, pekerjaan, asal negara, status pernikahan, hingga alamat email. Facebook melalui juru bicaranya telah mengonfirmasi perihal kebocoran data ini. Menurut juru bicara Facebook, ratusan juta data pengguna ini bocor karena adanya kerentanan keamanan yang dialami Facebook.[6] Pada tahun 2020, Tokopedia dilaporkan mengalami peretasan. Diperkirakan sejumlah 91 juta akun dan 7 juta akun *merchant* berhasil diambil data pribadinya oleh peretas. Pelaku menjual data di darkweb berupa user ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor telepon, dan password yang masih tersandi. Data pribadi tersebut dijual dengan harga US$5.000 atau sekitar Rp74 juta, bahkan ada 14.999.896 akun Tokopedia yang datanya saat ini bisa didownload.[7]

Berdasarkan pada kasus kebocoran data pribadi yang terjadi bahwa sejatinya data pribadi merupakan aset yang sangat berharga, karena data pribadi *as a new oil* sehingga perlunya perlindungan. Melihat pula kasus yang terjadi, maka dapat diketahui bahwa terjadinya kebocoran data pribadi telah mengakibatkan kerugian pada pengguna *platform*. Perlindungan data pribadi telah diatur secara khusus dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (selanjutnya disebut **UU PDP**). Pasal 1 angka 4 UU PDP mengatur bahwa perusahaan *e-commerce* digolongkan sebagai pengendali data pribadi yang berbentuk korporasi dan tunduk pada ketentuan pelindungan data pribadi dalam UU PDP.

Pasal 39 ayat (1) dan (2) UU PDP mewajibkan Pengendali data pribadi menerapkan sistem keamanan terhadap data pribadi, yang berbunyi "*pengendali data pribadi wajib mencegah data pribadi yang diakses secara tidak sah dengan menggunakan sistem keamanan terhadap data pribadi yang diproses dan/atau memproses data pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab*". Sistem keamanan tersebut adalah Sertifikat Keandalan. Ketentuan ini sejalan dengan Pasal 21 ayat (1) huruf e Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (selanjutnya

6 Galuh Putri Riyanto, "Data 533 Juta Pengguna Facebook Bocor, Termasuk Indonesia," Kompas.com, https://tekno.kompas.com/read/2021/04/04/09330067/data-533-juta-pengguna-facebook-bocor-termasuk-indonesia?page=all (diakses 16 Juli 2023).

7 Adhi Wicaksono, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual," CNN Indonesia, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual (diakses 17 Juli 2023).

disebut PP PMSE) yang mewajibkan pelaku usaha dalam negeri dan/atau luar negeri untuk memenuhi ketentuan persyaratan teknis yang ditetapkan oleh instansi terkait dan memperoleh Sertifikat Keandalan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 1 angka 27 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP PSTE) menjelaskan bahwa yang dimaksud Sertifikat Keandalan adalah dokumen yang menyatakan pelaku usaha yang menyelenggarakan transaksi elektronik telah lulus audit atau uji kesesuaian dari lembaga sertifikasi keandalan. Pasal 76 PP PSTE menjelaskan bahwa Sertifikat Keandalan yang diterbitkan oleh Lembaga Sertifikasi Keandalan meliputi kategori; a. registrasi identitas; b. keamanan Sistem Elektronik; dan c. kebijakan privasi. Pada bagian Penjelasan Pasal 76 huruf c dinyatakan bahwa. "*Kebijakan privasi merupakan Sertifikat Keandalan yang jaminan keandalannya adalah memberikan kepastian bahwa Data Pribadi konsumen dilindungi kerahasiaannya sebagaimana mestinya*."

Terkait penggunaan Sertifikat Keandalan antara UU PDP dan PP PMSE dengan UU ITE dan PP PSTE terdapat adanya perubahan "sifat norma". Dalam UU ITE dan PP PSTE, sifat norma terkait penggunaan Sertifikasi Keandalan hanyalah "mengatur", yaitu dengan digunakannya frasa "dapat" pada Pasal 10 UU ITE dan Pasal 42 ayat (2) PP PSTE. Sifat norma terkait penggunaan Sertifikat Keandalan berubah secara drastis pada UU PDP dan PP PMSE menjadi "memaksa", yaitu dengan digunakannya frasa "wajib" pada Pasal 39 ayat (1) dan (2) UU PDP[8] dan Pasal 21 ayat (1) huruf e PP PMSE.

Sebagai pelaku usaha *e-commerce* memiliki kewajiban untuk melindungi data pribadi konsumennya dari kemungkinan kebocoran data sebagaimana ketentuan dalam UU PDP dan PP PMSE yang mewajibkan pelaku usaha *e-commerce* untuk menerapkan penggunaan Sertifikat Keandalan sebagai bentuk kebijakan privasi untuk menjamin kerahasiaan sebagaimana mestinya. Namun, pada praktiknya tidak semua pelaku usaha *e-commerce* di Indonesia menggunakan Sertifikat Keandalan yang dimaksud untuk mematuhi ketentuan pelindungan data pribadi. Sertifikat Keandalan tersebut adalah Sertifikat Keandalan Privasi.

Oleh karena hal tersebut, sesuai dengan kewajiban yang telah ditetapkan dalam UU PDP dan PP PMSE terkait penggunaan Sertifikat Keandalan Privasi pada pelaku usaha *e-commerce,* maka hal ini perlu dikaji lebih dalam terkait bagaimana pelaksanaan kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* di Indonesia, serta bagaimana pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya kebocoran data pribadi pengguna berdasarkan hukum positif Indonesia. Oleh sebab itu, harapan penulis dengan dilaksanakannya penelitian ini dapat memberikan edukasi dan pemahaman bagi pembaca dan masyarakat terkait kewajiban

[8] Muhammad Amirulloh, "Kewajiban Sertifikat Keandalan dalam UU PDP: Bukti Pelindungan Data Pribadi dalam Sistem Elektronik," Universitas Padjadjaran https://blogs.unpad.ac.id/muhamadamirulloh/2022/12/29/kewajiban-sertifikat-keandalan-dalam-uu-pdp-bukti-pelindungan-data-pribadi-dalam-sistem-elektronik/ (diakses pada 16 Juli 2023).

penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* di Indonesia disertai dengan pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya kebocoran data pribadi pengguna berdasarkan peraturan perundang-undangan yang berlaku di Indonesia.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif, artinya penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan kepustakaan atau data sekunder saja.[9] Penulisan ini mengkaji pokok-pokok permasalahan berkaitan dengan pelindungan data pribadi dengan menggunakan pendekatan perundang-undangan (*statute approach*)[10] yang berkaitan dengan isu hukum yang diteliti. Fokus penelitian berpusat pada pelaksanaan kewajiban penggunaan Sertifikat Keandalan oleh pelaku usaha *e-commerce* di Indonesia dan pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya kebocoran data pribadi pengguna berdasarkan hukum positif Indonesia, utamanya ditinjau dari bahan hukum primer berupa Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, bahan hukum sekunder berupa buku-buku serta jurnal penelitian terdahulu, dan bahan hukum tersier berupa artikel ilmiah. Adapun teknik pengumpulan data dengan menggunakan penelitian kepustakaan serta penelusuran data daring. Dengan demikian, rancangan analisis yang dibuat oleh penulis akan berhubungan dengan peraturan perundang-undangan yang berlaku yang dikaitkan pada fakta hukum di lapangan. Sehingga, analisis ini dapat menjadi dasar untuk menjawab persoalan atas kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku *usaha e-commerce* sebagai bentuk pelindungan konsumen.

C. Pembahasan

1. Pelaksanaan kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* di Indonesia

Dalam rangka pelaksanaan transaksi elektronik, seluruh pelaku usaha *e-commerce* wajib untuk memberikan jaminan pelindungan data pribadi konsumen sebagaimana ditetapkan dalam Pasal 39 UU PDP dan Pasal 21 dan Pasal 24 PP PMSE, dimana seluruh pelaku usaha *e-commerce* terikat dalam suatu kewajiban untuk melindungi data pribadi konsumennya dengan menyediakan sebuah pengaturan kebijakan privasi. Pada praktiknya, beberapa pelaku usaha *e-commerce* telah mematuhi ketentuan tersebut dengan membuat suatu kebijakan privasi untuk mencegah terjadinya kebocoran data pribadi. Kebijakan privasi tersebut dapat berupa peraturan tertulis yang ditujukkan kepada pengguna *platform* yang diintegrasikan ke

[9] Soerjono Soekanto dan Sri Mahmudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat* (Jakarta: Raja Grafindo Persada, 2003), hlm. 13.
[10] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Penerbit Kencana, 2007), hlm. 96.

dalam bentuk *e-contract* serta penggunaan Sertifikat Keandalan Privasi sebagaimana yang telah diwajibkan dalam UU PDP dan PP PMSE.

Adapun dalam pembahasan ini, penulis akan menjelaskan pentingnya penggunaan Sertifikat Keandalan Privasi sebagai bentuk kewajiban pelaku usaha *e-commerce* dalam melindungi data pribadi pengguna di Indonesia, yaitu sebagai berikut:

a. Facebook *Marketplace*

Mark Zuckerbeg selaku pencipta sekaligus CEO Facebook mengumumkan secara resmi perubahan nama Facebook menjadi Meta. Namun perubahan ini ditujukan kepada perusahaan induk, sehingga Meta adalah nama resmi dari perusahaan Facebook. Meta adalah perusahaan yang menaungi Facebook, Messenger, Instagram, dan Whatsapp.[11] *Platform* Facebook tidak hanya menyediakan layanan menghubungkan pertemanan (media sosial), akan tetapi juga menyediakan layanan *e-commerce*, yang dikenal dengan Facebook *Marketplace.* Perubahan nama perusahaan induk ini mengakibatkan terhubungnya secara luas antara pengguna Facebook dengan pihak lain selain pengguna Facebook. Setelah diumumkan secara resmi perubahaan nama perusahaan induk ini, beberapa orang termasuk pengguna Facebook merasa khawatir termasuk membahas kembali isu kebocoran data pribadi pengguna.

Hal ini menjadi fokus utama Facebook *Marketplace* dalam hal melindungi data pribadi pengguna yakni dengan dibuatnya suatu kebijakan privasi yang diketahui hanya menjelaskan seputar cara *platform* mengumpulkan, menggunakan, dan membagikan informasi privasi.

1) Perolehan dan Pengumpulan Data Pengguna

Bentuk komitmen nyata Facebook *Marketplace* 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, pengaksesan, atau mempergunakan layanan pada *platform*. Akan tetapi, terdapat beberapa kebijakan privasi dari Facebook *Marketplace* yang memiliki kelemahan dan dapat berpotensi menimbulkan kebocoran data pribadi pengguna, yakni dengan memberikan ID pengguna kepada pengiklan bersama dengan data pada aktivitas pengguna, dengan mengizinkan pihak ketiga untuk mengakses penuh ke data pribadi pengguna, dan dengan tidak menghapus beberapa data pengguna ketika pengguna menghapus akun.

Selanjutnya, dinyatakan bahwa Facebook *Marketplace* dapat mengumpulkan informasi data pribadi meskipun tidak memiliki akun. Diketahui pula bahwa Facebook *Marketplace* menggunakan data pribadi yang dikumpulkan untuk memberikan pengalaman yang dipersonalisasi kepada pengguna, termasuk iklan, bersama dengan tujuan lain yakni untuk mengakses dan meninjau informasi pengguna. Selanjutnya dinyatakan bahwa Facebook *Marketplace* dapat menggabungkan data

[11] Aditia Lestari, "Facebook Resmi Ganti Nama Jadi Meta, Apa Saja Dampak dan Perubahannya Pada Produk Layanan?," Kapanlagi,com https://plus.kapanlagi.com/facebook-resmi-ganti-nama-jadi-meta-apa-saja-dampak-dan-perubahannya-pada-produk-layanan-074f32.html (diakses 17 Juli 2023).

yang diperoleh dari sumber tersebut dengan data lain.[12]

Pada tahun 2022, diketahui bahwa terdapat kelemahan dalam sistem manajemen datanya, yang mengakui bahwa mereka bingung kemana data penggunanya pergi. Kebocoran terungkap setelah perusahaan yang mengubah nama perusahaannya menjadi Meta mendapat kecaman karena mengumpulkan informasi pribadi pengguna tanpa disadari untuk tujuan termasuk iklan bertarget.[13] Oleh karena hal tersebut dengan tidak dijelaskan secara spesifik terkait penggabungan data lain berkenaan dengan mekanisme dan jenis data yang digabungkan, maka hal ini dapat memicu lahirnya pengolahan data yang bermasalah.

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.

2) Pentransferan Informasi Pribadi

Dalam kebijakan privasi pada *platform* Facebook *Marketplace,* dijelaskan bahwa informasi pribadi akan ditransfer atau dikirim ke atau disimpan dan diproses di pusat, termasuk Amerika Serikat, Irlandia, Denmark dan Swedia sebagai negara tempat Meta *Company Products* tersedia, hal ini dilakukan karena Meta bersifat global, dengan pengguna, mitra, dan karyawan di seluruh dunia, sehingga diperlukannya transfer informasi pribadi, demikian cara pengguna dapat terhubung dengan publik.

Mengingat sifatnya yang global dan dapat terhubung dengan publik di seluruh dunia, maka perlunya perlindungan pribadi yang ketat untuk mencegah terjadinya pengaksesan informasi/data pribadi secara tidak sah. Dalam hal ini, Facebook *Marketplace* menyebutkan bahwa "*kami mengandalkan mekanisme yang tepat untuk transfer data internasional, kami juga memastikan bahwa perlindungan yang tepat tersedia setiap kali kami mentransfer informasi anda. Misalnya, kami mengenkripsi informasi anda saat transit melalui jaringan publik untuk melindunginya dari akses tidak sah*." Dapat dilihat terkait kebijakan tersebut, maka ditemukan adanya kelemahan terkait pelindungan data pribadi pengguna *platform* tersebut, dimana tidak diatur dan dijelaskan bagaimana cara *platform* mengenkripsi informasi pribadi pengguna, dan bagaimana cara memastikan bahwa data yang ditransfer ke negara lain terjamin keamanannya. Padahal hal-hal tersebut sangat penting diatur untuk keamanan data pribadi konsumen dalam bertransaksi.[14]

Demikian, diketahui bahwa kebijakan privasi pada *platform* Facebook *Marketplace* sejatinya masih kurang optimal dan belum menerapkan penggunaan Sertifikat Keandalan Privasi yang merupakan sistem keamanan elektronik sebagaimana diwajibkan dalam

---

12 Meta Kebijakan Privasi, "Apa yang dimaksud Kebijakan Privasi dan apa yang dicakup di dalamnya?," Facebook https://id-id.facebook.com/privacy/policy/?entry_point=facebook_page_footer (diakses 17 Juli 2023).

13 Natalia Endah Hapsari, "Facebook Ganti Rugi Kebocoran Data Pengguna, Bagaimana Caranya?," Republika.co.id https://tekno.republika.co.id/berita/rtcrli478/facebook-ganti-rugi-kebocoran-data-pengguna-bagaimana-caranya (diakses 17 Juli 2023).

14 Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law (Aspek Hukum Teknologi Informasi)* (Bandung: Refika Aditama, 2005), hlm. 157.

UU PDP dan PP PMSE, sehingga rentan mengakibatkan terjadinya pengaksesan data pribadi secara tidak sah yang memicu kebocoran data pribadi. Mengingat pengguna *platform* Facebook *Marketplace* terbilang banyak yakni 1 miliar di dunia yang termasuk 119,9 juta pengguna di Indonesia, maka perlunya pelindungan data pribadi yang ketat seperti yang telah diwajibkan dalam Pasal 39 UU PDP yakni pelaku usaha *e-commerce* wajib mencegah data pribadi diakses secara tidak sah dengan menggunakan sistem keamanan terhadap data pribadi yakni Sertifikat Keandalan Privasi. Pasal 21 dan Pasal 24 PP PMSE juga mewajibkan hal yang sama terkait kewajiban penggunaan Sertifikat Keandalan Privasi sebagai upaya untuk membangun kepercayaan terhadap sistem yang diselenggarakannya kepada publik dan untuk mencegah serta penanggulangan terhadap kebocoran data pribadi yang merugikan pengguna *platform*. Penggunaan Sertifikat Keandalan Privasi ini pada dasarnya sudah diterapkan oleh *platform* Tokopedia sejak tahun 2021 sebagai pelaku usaha *e-commerce* yang sudah menggunakan Sertifikat Keandalan Privasi ISO/IEC 27701 *Privacy Information Management* dari *British Standards Institution (BSI)* yang dapat dilihat pada bagian paling bawah laman Tokopedia.

b. Tokopedia

Belajar dari kegagalan dalam hal menjaga dan melindungi data pribadi pengguna, Tokopedia merubah kebijakan privasinya untuk menjamin pelindungan data pribadi pengguna. Tokopedia menggunakan Sertifikat Keandalan Privasi ISO/IEC 27701 *Privacy Information Management* dari *British Standards Institution (BSI)* yang dapat dilihat pada bagian paling bawah laman Tokopedia. Penggunaan sertifikat keandalan privasi oleh Tokopedia sejak tahun 2021 hingga 2024, dengan menggunakan Sertifikat Keandalan Privasi, Tokopedia dapat dipercaya atau diyakini aman ketika konsumen melakukan pertukaran data dalam *platform* tersebut.

Jika logo Sertifikat Keandalan Privasi ini diklik, maka langsung terarahkan ke dalam isi dari Sertifikat Keandalan Privasi ISO/IEC 27701 *Privacy Information Management* dari *British Standards Institution (BSI)*, dimana dalam Sertifikat Keandalan Privasi ini menjelaskan ruang lingkup yang dilindungi, sertifikat/nomor lisensi, serta tenggat waktu berlakunya Sertifikat Keandalan Privasi ISO/IEC 27701. Dengan menggunakan Sertifikat Keandalan Privasi, maka secara tidak lansgung telah menjamin keamanan data pribadi penyelenggara sistem elektronik, dengan istilah lainnya adalah pemberian kepercayaan terhadap pelaku usaha yang menyelenggarakan transaksi elektronik. Sertifikat Keandalan Privasi juga bertujuan untuk melindungi data pribadi konsumen dalam melakukan transaksi elektronik dan juga merupakan jaminan bahwa pelaku usaha *e-commerce* telah memenuhi kriteria yang ditentukan oleh lembaga sertifikasi keandalan.[15] Sehingga, para pengguna tidak lagi khawatir terkait data pribadi yang diberikan kepada pelaku usaha *e-commerce*. Menurut Endang Sri Wahyuni, penggunaan Sertifikat Keandalan Privasi lebih efektif menjamin pelindungan konsumen dibandingkan dengan perlindungan konsumen yang didasarkan

[15] Pasal 74 ayat (1) dan ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

pada peraturan perundang-undangan, karena pelaku usaha *e-commerce* yang telah menggunakan Sertifikat Keandalan Privasi memberikan jaminan kepada konsumen bahwa keamanan data pribadi yang diberikan oleh konsumen ke pelaku usaha *e-commerce* telah memenuhi syarat standar keamanan.[16]

Adapun bentuk kebijakan privasi lainnya adalah berupa penyamaran informasi pembeli di beberapa halaman tertentu, kebijakan ini berlaku mulai pada tanggal 28 November 2022 bahwa informasi yang mencakup nama pembeli dan penerima, nomor telepon, dan alamat pengiriman disamarkan sebagian di beberapa halaman tertentu.[17] Kebijakan privasi ini ditetapkan sesuai dengan UU PDP yang telah diundangkan per 17 Oktober 2022 lalu, serta komitmen Tokopedia dalam upaya perlindungan data pengguna. Pembatasan akses data pribadi pembeli ini merupakan tindak lanjut dari upaya yang sudah dilakukan Tokopedia selama ini dalam memperkuat perlindungan data pengguna Tokopedia serta memberikan pengalaman belanja yang lebih aman dan nyaman. Tanpa disadari, bahwa upaya pembaharuan kebijakan privasi oleh Tokopedia selaku pelaku usaha *e-commerce* merupakan upaya preventif untuk mencegah terjadinya kebocoran data pribadi pengguna sesuai dengan UU PDP dan PP PMSE.

Selain melindungi pengguna dari pengaksesan data pribadi secara tidak sah, dengan menggunakan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* juga tentunya memberikan perlindungan khusus terhadap pelaku usaha *e-commerce*, seperti pembatasan tanggung jawab terjadinya pengaksesan data pribadi secara tidak sah. Dalam hal pembatasan tanggung jawab pelaku usaha *e-commerce* dikenal dengan prinsip *Safe Harbour*. Mengapa pembatasan tanggung jawab ini dapat diberikan pada pelaku usaha *e-commerce*? Menurut penulis, pembatasan tanggung jawab ini diberikan kepada pelaku usaha yang sudah menerapkan kewajibannya sesuai dengan Pasal 39 UU PDP dan Pasal 21 dan Pasal 24 PP PMSE dalam hal upaya pencegahan terjadinya pengaksesan data pribadi secara tidak sah, artinya kegagalan ini terjadi di luar kehendak pelaku usaha *e-commerce.* Namun disisi lain, mengingat upaya pencegahan yang dilakukan oleh pelaku usaha *e-commerce* telah sesuai sebagaimana diwajibkan dalam Pasal 39 UU PDP dan Pasal 21 dan Pasal 24 PP PMSE, maka jika terjadi kegagalan seperti pengaksesan data pribadi secara tidak sah oleh pihak diluar pelaku usaha *e-commerce,* pembatasan tanggung jawab ini wajib diberikan kepada pelaku usaha *e-commerce.* Pembatasan tanggung jawab ini bukan berarti melepaskan tanggung jawab, akan tetapi dalam hal melakukan tanggung jawab atas terjadinya kegagalan pelindungan data pribadi pelaku usaha *e-commerce* mempunyai batasan tanggung jawab. Artinya pelaku usaha e-commerce dengan pembatasan tanggung jawab ini akan bebas dari tuduhan yang dibuat oleh *merchant.*[18]

---

16 Endang Sri Wahyuni, *Aspek Hukum Sertifikasi & Keterkaitannya Dengan Perlindungan Konsumen* (Bandung: Citra Aditya Bakti, 2003), hlm. 177.

17 Tokopedia Pusat Edukasi Seller, "Penerapan Kebijakan Pelindungan Data Pembeli," Tokopedia https://seller.tokopedia.com/edu/kebijakan-data-pembeli/ (diakses 17 Juli 2023).

18 Bintoro Agung, "Kebijakan Safe Harbour, Tanggung Jawab E-Commerce 'Dibatasi'," CNN Indonesia https://www.cnnindonesia.com/teknologi/20170227142956-185-196481/kebijakan-safe-harbour-tanggung-jawab-e-commerce-dibatasi (diakses 18 Juli 2023).

2. Pertanggungjawaban pelaku usaha *e-commerce* dalam hal kebocoran data pribadi pemilik akun berdasarkan hukum positif di Indonesia

Kebocoran data pribadi yang diproses ataupun dikelola oleh pelaku usaha *e-commerce,* baik karena peretasan pihak ketiga ataupun secara sengaja dibocorkan kepada pihak ketiga atau publik, merupakan tanggung jawab pelaku usaha *e-commerce* selaku pengendali data pribadi. Mengingat Pasal 39 UU PDP serta Pasal 21 dan Pasal 24 PP PMSE telah mewajibkan pelaku usaha *e-commerce* untuk menggunakan sistem keamanan elektronik yang aman, andal, terpercaya guna mencegah terjadinya pengaksesan data pribadi secara tidak sah, maka terhadap pelaku usaha *e-commerce* yang tidak memenuhi ketentuan sebagaimana diwajibkan dalam pasal tersebut wajib untuk bertanggung jawab atas terjadinya kebocoran data pribadi.

Menilik upaya pencegahan yang dilakukan oleh *platform* Facebook *Marketplace*, yang dimana belum memenuhi ketentuan sebagaimana diwajibkan oleh UU PDP dan PP PMSE untuk mencegah terjadinya pengaksesan data pribadi secara tidak sah, maka *platform* Facebook *Marketplace* wajib bertanggung jawab penuh atas terjadinya kebocoran data pribadi. UU PDP dan PP PMSE telah mewajibkan kepada seluruh pelaku usaha *e-commerce* untuk memperoleh dan menggunakan Sertifikat Keandalan Privasi untuk melindungi data pribadi konsumennya dari kemungkinan kebocoran data dan menjamin kerahasiaan sebagaimana mestinya. Apabila terdapat kegagalan dalam hal melindungi data pribadi pengguna, maka *platform* tersebut wajib bertanggung jawab dan tidak akan bebas dari tuduhan *merchant*, artinya tidak mendapatkan perlindungan khusus seperti pembatasan tanggung jawab oleh pelaku usaha *e-commerce*. Sebagaimana Pasal 47 UU PDP bahwa pelaku usaha *e-commerce* selaku pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan data pribadi.

Mengenai pertanggungjawaban oleh pelaku usaha *e-commerce* atas terjadinya kegagalan dalam hal melindungi data pribadi pengguna, maka untuk menjawab hal ini perlu melihat dua prinsip pertanggungjawaban pelaku usaha *e-commerce*, sebagai berikut:

a) Strict Liabilty

Prinsip tanggung jawab mutlak (*strict liability*) dapat diartikan bahwa pelaku usaha *e-commerce* harus bertanggung jawab atas kerugian konsumen tanpa harus membuktikan ada tidaknya kesalahan pada dirinya.[19] 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.[20] Namun,

[19] Yudha Hadian Nur dan Dwi Wahyuniarti Prabowo, "Penerapan Prinsip Tanggung Jawab Mutlak (Strict Liability) Dalam Rangka Perlindungan Konsumen," Buletin Ilmiah Litbang Perdagangan, Vol. 5 No. 2 (2011): 178.
[20] Sidharta, *Hukum Perlindungan Konsumen Indonesia* (Jakarta: PT Grasindo, 2000), hlm. 63.

apakah tepat jika pelaku usaha *e-commerce* telah memenuhi ketentuan sebagaimana yang diwajibkan dalam UU PDP dan PP PMSE dalam hal upaya pencegahan pengaksesan data pribadi secara tidak sah? Menurut penulis, prinsip *strict liability* ini tidak tepat diberikan kepada pelaku usaha *e-commerce* untuk melaksanakan pertanggungjawaban atas kegagalan pelindungan data pribadi penggunanya, karena dalam Surat Edaran Menteri Komunikasi dan Informasi No. 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia *Platform* dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk *User Generated Content*, dinyatakan bahwa penyedia *platform* sebagai Penyelenggara Sistem Elektronik bertanggungjawab terhadap penyelenggaraan sistem elektroniknya yakni dengan menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Ketentuan pertanggungjawaban tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian dari pihak pengguna sistem elektronik. Dalam Surat Edaran ini pelaku usaha *e-commerce* yang telah memenuhi kewajibannya dengan membuat suatu kebijakan privasi berupa Sertifikat Keandalan Privasi sebagaimana diwajibkan dalam UU PDP dan PP PMSE maka wajib melaksanakan batasan dan tanggung jawab atau yang dikenal dengan prinsip *safe harbour.*

b) Safe Harbour

Menurut Black's Law Dictionary, *safe harbour* adalah *the provision in a law or agreement that will protect from any liability or penalty as long as set conditions have been met,* jika diterjemahkan ke dalam Bahasa Indonesia *safe harbour* adalah ketentuan dalam undang-undang atau perjanjian yang akan melindungi dari segala kewajiban atau hukuman, selama syarat-syarat yang ditetapkan telah dipenuhi.[21] Prinsip *Safe Harbour* dapat pula diartikan sebagai pembatasan tanggung jawab bagi pelaku usaha *e-commerce* apabila telah melaksanakan langkah-langkah pencegahan atau penanganan jika terjadi pengaksesan data pribadi secara tidak sah dan mengakibatkan kebocoran data pribadi pengguna di *platform*nya. Terhadap pelaku usaha *e-commerce* yang telah memenuhi langkah-langkah pencegahan atau penanganan atas kebocoran data pribadi sebagaimana yang telah diwajibkan dalam UU PDP dan PP PMSE yakni mewajibkan untuk menggunakan Sertifikat Keandalan Privasi pada *platform*nya serta membuat kebijakan privasi sebagai bentuk pelindungan data pribadi pengguna *platform,* maka pelaku usaha *e-commerce* tersebut tentunya diberikan pelindungan khusus, seperti pembatasan tanggung jawab terjadinya pengaksesan data pribadi secara tidak sah sebagaimana diatur dalam Surat Edaran Menteri Komunikasi dan Informasi No. 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia *Platform* dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik (*Electronic Commerce*).

[21] Prof. Dr. Ahmad M Ramli, "Konten Medsos Tak Terkendali, "Safe Harbour" Digugat agar Tak Absolut," Kompas.com https://www.kompas.com/tren/read/2022/12/13/175705465/konten-medsos-tak-terkendali-safe-harbour-digugat-agar-tak-absolut?page=all (diakses 17 Juli 2023).

Jika pada analisis di atas berdasarkan pada prinsip pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya pengaksesan data pribadi secara tidak sah, maka selanjutnya penulis akan membahas pertanggungjawaban pelaku usaha *e-commerce* atas kasus kebocoran data menurut hukum positif Indonesia, sebagai berikut:

a. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Dalam Pasal 1 angka 4 *jo.* Pasal 1 angka 7 UU PDP menjelaskan bahwa pelaku usaha *e-commerce* digolongkan sebagai pengendali data pribadi yang berbentuk korporasi yang tunduk pada ketentuan pelindungan data pribadi dalam UU PDP. Dalam hal melakukan pemrosesan data pribadi, pelaku usaha *e-commerce* harus memperhatikan beberapa prinsip pelindungan data pribadi sebagaimana diatur dalam Pasal 16 ayat (2) UU PDP yang meliputi:

a. Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;
b. Pemrosesan data pribadi dilakukan sesuai dengan tujuannya;
c. Pemrosesan data pribadi dilakukan dengan menjamin hak subjek data pribadi;
d. Pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
e. Pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan, pengungkapan, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan data pribadi;
f. Pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan pelindungan data pribadi;
g. Data pribadi dimusnahkan/dihapus setelah masa retensi berakhir berdasarkan permintaan subjek data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
h. Pemrosesan data pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.

Berdasarkan ketentuan di atas, pada dasarnya pelaku usaha *e-commerce* mempunyai kewajiban untuk mencegah kebocoran data pribadi dengan melindungi keamanan data pribadi dari pengaksesan, pengungkapan, pengubahan yang tidak sah, penyalahgunaan, perusakan dan penghilangan data pribadi. Pasal 39 UU PDP juga menegaskan bahwa pencegahan sebagaimana yang dimaksud dilakukan dengan menggunakan sistem keamanan terhadap data pribadi yakni Sertifikat Keandalan Privasi. Jika terjadi kebocoran data pribadi, maka perusahaan *e-commerce* yang bersangkutan wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada penggunanya dan lembaga yang menyelenggarakan data pribadi.[22] Pemberitahuan tersebut harus memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi tersebut bocor, serta upaya penanganan serta pemulihan kebocoran data pribadi.[23] Jika kebocoran data pribadi tersebut

[22] Pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[23] Pasal 46 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

hingga mengganggu pelayanan publik dan/ atau berdampak serius terhadap kepentingan masyarakat, maka perusahaan *e-commerce* harus mengumumkan kebocoran tersebut kepada masyarakat.[24]

Adapun sanksi administratif sebagaimana diatur dalam Pasal 57 ayat (1) UU PDP yang akan dikenai kepada pelaku usaha *e-commerce* apabila terjadi kebocoran data pribadi, yakni berupa; (a) peringatan tertulis; (b) penghentian sementara kegiatan pemrosesan data pribadi; (c) penghapusan atau pemusnahan data pribadi; (d) denda administratif paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran (Pasal 57 ayat (3) UU PDP). Sanksi administratif ini diberikan kepada pelaku usaha *e-commerce* apabila melakukan pelanggaran terhadap ketentuan, salah satunya adalah Pasal 39 ayat (1) yakni kewajiban pelaku usaha *e-commerce* untuk mencegah data pribadi diakses secara tidak sah dengan menggunakan sistem keamanan terhadap data pribadi, yaitu Sertifikat Keandalan Privasi.[25]

Dalam hal terjadi kebocoran data pribadi pada suatu *platform marketplace*, pengguna selaku konsumen *platform marketplace* yang menjadi korban kebocoran data pribadi dapat menyelesaikan sengketa ini melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan.[26] Terhadap pelaku usaha yang telah melanggar ketentuan sebagaimana dimaksud pada Pasal 39 UU PDP, yakni tidak melakukan pencegahan dengan menerapkan sistem keamanan elektronik berupa Sertifikat Keandalan Privasi, sehingga mengakibatkan pengaksesan data pribadi secara tidak sah, maka konsumen (dhi. pengguna *platform*) dapat mengajukan laporan kepada Lembaga Pelindungan Data Pribadi untuk menindak lanjuti pelaku usaha sesuai Pasal 70 UU PDP yaitu dikenakannya pidana denda paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan[27], selain itu pelaku usaha *e-commerce* dapat dijatuhi pidana tambahan berupa (a) perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana; (b) pembekuan seluruh atau sebagian usaha korporasi; (c) pelarangan permanen melakukan perbuatan tertentu; (d) penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan korporasi; (e) melaksanakan kewajiban yang telah dilalaikan; (f) pembayaran ganti kerugian; (g) pencabutan izin; dan/atau (h) pembubaran korporasi.[28]

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

Merujuk pada Pasal 100 ayat (2) PP PSTE menjelaskan bahwa bentuk pertanggungjawaban pelaku usaha *e-commerce* pada kasus kebocoran data yakni berupa sanski administrasi, yang terdiri atas denda administratif, diputuskannya akses, teguran tertulis, penghentian sementara,

[24] Pasal 46 ayat (3) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
[25] Pasal 57 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
[26] Pasal 64 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
[27] Pasal 70 ayat (3) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
[28] Pasal 70 ayat (4) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

maupun dikeluarkan dari daftar. Sanksi administratif ini diberikan kepada pelaku usaha e-commerce apabila melakukan pelanggaran administratif, salah satunya terhadap pelaku usaha *e-commerce* yang tidak melaksanakan ketentuan sebagaimana diwajibkan dalam Pasal 51 ayat (1) PP PSTE yakni kewajiban memiliki Sertifikat Elektronik yang dalam hal ini adalah Sertifikat Keandalan Privasi.

Sanksi administratif dikenakan pula kepada pelaku usaha *e-commerce* apabila melanggar ketentuan sebagaimana diatur dalam Pasal 14 ayat (1) PP PSTE terkait kewajiban pelaku usaha *e-commerce* melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi, yang meliputi:

a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik Data Pribadi;
b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
c. pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi;
d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi;
e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi;
f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan
g. pemrosesan Data Pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

Selain itu, sanksi administratif ini juga berlaku pada pelaku usaha yang melanggar ketentuan Pasal 14 ayat (5) PP PSTE. Namun, jika mencermati ketentuan sebagaimana diatur dalam Pasal 14 ayat (5) PP PSTE yang berbunyi "*Jika terjadi kegagalan dalam pelindungan data pribadi yang dikelolanya, penyelengara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut*" maka ditemukan kelemahan dalam hal pemberian pemberitahuan kepada pemilik data pribadi jika terjadi kegagalan dalam pelindungan data pribadi, dimana dalam pasal ini tidak dijelaskan waktu/durasi pemberitahuan secara tertulis kepada pemilik data pribadi. Dengan kata lain, apabila terjadi kebocoran data, maka pelaku usaha *e-commerce* dapat memberitahukan secara tertulis kapan saja, bahkan setelah keluarnya gugatan. Dapat dikatakan bahwa, beberapa pengaturan dalam PP PSTE masih belum mengatur secara jelas dan efektif untuk menanggulangi kebocoran data terutama dalam memberikan jaminan pelindungan kepada konsumen.

Dalam hal penyelesaian sengketa, PP PSTE tidak mengatur upaya yang dapat dilakukan korban kebocoran data pribadi (dhi. konsumen/pengguna *platform*) untuk menyelesaikan sengketa ini, seperti yang diatur pada UU PDP dan PP PMSE. Oleh karena itu, ketentuan yang diatur oleh PP PSTE masih belum optimal dan tidak adanya kepastian, sehingga belum cukup kuat menjadi payung

hukum pada kasus kebocoran data pribadi di *platform marketplace* Indonesia.

c. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

Pasal 14 PP PMSE mewajibkan pelaku usaha dalam negeri dan/atau luar negeri menggunakan sistem elektronik yang memiliki sertifikat kelayakan sistem elektronik sesuai dengan ketentuan peraturan perundang-undangan. Hal ini ditegaskan dalam Pasal 21 ayat (1) huruf e PP PMSE mewajibkan pelaku usaha dalam negeri dan/atau luar negeri untuk memenuhi ketentuan persyaratan teknis yang ditetapkan oleh instansi terkait dan memperoleh Sertifikat Keandalan sesuai dengan ketentuan peraturan perundang-undangan. Dalam hal mencegah terjadinya pengaksesan data pribadi secara tidak sah, maka diwajibkan kepada pelaku usaha *e-commerce* memperoleh Sertifikat Keandalan Privasi. Sertifikat Keandalan Privasi ini digunakan oleh pelaku usaha *e-commerce* untuk membangun keterpercayaan terhadap sistem yang diselenggarakannya kepada publik sebagaimana ketentuan Pasal 24 PP PMSE. Untuk meningkatkan pelindungan terhadap konsumen, pelaku usaha wajib menyediakan layanan pengaduan bagi konsumen.[29] Dalam hal pelaku usaha *e-commerce* merugikan konsumen, konsumen dapat melaporkan kerugian yang diderita kepada Menteri.[30] Jika pelaku usaha *e-commerce* tidak menyelesaikan pelaporan, maka pelaku usaha *e-commerce* akan masuk ke dalam daftar prioritas pengawasan oleh Menteri.[31]

Adapun bentuk pertanggungjawaban pelaku usaha *e-commerce* apabila melanggar ketentuan sebagaimana diatur dalam Pasal 80 ayat (1) PP PMSE, diantaranya Pasal 21, Pasal 23, dan Pasal 24 PP PMSE, yang dimana dalam ketentuan pasal tersebut mewajibkan pelaku usaha *e-commerce* untuk memperoleh Sertifikat Keandalan Privasi guna mencegah dan menanggulangi terjadinya pengaksesan data pribadi secara tidak sah, maka terhadap pelaku usaha *e-commerce* yang melanggar ketentuan tersebut dikenai sanksi administratif berupa; (a) peringatan tertulis, (b) dimasukkan dalam daftar prioritas pengawasan; (c) dimasukkan dalam daftar hitam; (d) pemblokiran sementara layanan PPMSE dalam negeri dan/atau PPMSE luar negeri oleh instansi terkait yang berwenang; dan/atau (e) pencabutan izin usaha.

Menilik ketentuan yang diatur oleh pasal tersebut, penulis berpandangan bahwa pada dasarnya ketentuan yang diatur oleh PP PMSE sejatinya bertujuan untuk meningkatkan kepercayaan dan jaminan pelindungan data pribadi konsumen. Terlebih cakupan pelaku usaha yang diatur dalam PP PMSE berskala nasional sampai internasional, sehingga dapat mengurangi rasa kekhawatiran pemilik data pribadi untuk mengirimkan dan/atau bertukar data pribadi kepada pelaku usaha *e-commerce* tersebut. Namun, sayangnya pertanggungjawaban pelaku usaha *e-commerce* yang diatur dalam PP PMSE masih kurang tegas dan belum dewasa, dimana penjatuhan denda kepada pelaku usaha *e-commerce* yang melanggar ketentuan sebagaimana diatur pada pasal tersebut tidak

[29] Pasal 27 Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik
[30] Pasal 18 ayat (1) Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik
[31] Pasal 18 ayat (3) Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

diatur, sehingga ketidaktegasan ini dapat menjadi celah pelaku usaha *e-commerce* dalam berdalih dan melepas tanggung jawabnya atas kelalaian yang terjadi.

Dalam hal terjadi kebocoran data pribadi dalam PMSE, para pihak dapat menyelesaikan sengketa melalui pengadilan atau melalui mekanisme penyelesaian sengketa lainnya[32], Penyelesaian sengketa PMSE dalam hal ini kebocoran data pribadi dapat diselenggarakan secara elektronik (*online dispute resolution*) sesuai dengan ketentuan peraturan perundang-undangan.[33]

D. Penutup

Berdasarkan hasil penelitian yang telah dilakukan, maka penulis memperoleh kesimpulan bahwa pelaksanaan kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* di Indonesia belum semuanya menggunakan Sertifikat Keandalan Privasi. *Platform* Tokopedia adalah pelaku usaha *e-commerce* yang telah memenuhi ketentuan tersebut dan menggunakan Sertifikat Keandalan Privasi ISO/IEC 27701 dari *British Standards Institution* (BSI) untuk melindungi data pribadi penggunanya. Hukum positif di Indonesia juga belum semuanya tegas dan belum mengatur secara eksplisit terkait penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce.* Sejatinya, pertanggungjawaban pelaku usaha *e-commerce* dalam hal terjadinya kebocoran data pribadi mengedepankan prinsip *safe harbour.* Mengingat UU PDP dan PP PMSE telah mewajibkan penggunaan Sertifikat Keandalan Privasi untuk mencegah dan menangani terjadinya pengaksesan data pribadi secara tidak sah, maka kepada pelaku usaha yang belum menggunakan Sertifkat Keandalan Privasi tidak berhak untuk mendapatkan pembatasan tanggung jawab sebagai perlindungan khusus. Pengaturan mengenai pertanggungjawaban pelaku usaha *e-commerce* atas kebocoran data pribadi oleh PP PSTE dan PP PMSE belum diatur secara eksplisit, sehingga dianggap tidak tegas dan tidak efisien untuk diimplementasikan. Namun, mengingat Indonesia sudah memiliki UU PDP, maka dapat menjadi payung hukum untuk melindungi korban atas kebocoran data pribadi. Pengguna selaku konsumen *platform marketplace* yang menjadi korban kebocoran data pribadi dapat menyelesaikan sengketa ini melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan.

Adapun, secara preventif pemerintah harus mengatur kewajiban penggunaan Sertifikat Keandalan Privasi oleh pelaku usaha *e-commerce* secara tegas dan eksplisit. Menurut penulis, hal ini menjadi penting untuk diatur dalam undang-undang, peraturan pemerintah serta peraturan turunan lainnya agar dapat memberikan regulasi yang jelas dan terarah sehingga dapat menciptakan kepastian hukum. Kemudian, perlu juga dilakukan pengharmonisasian antara PP PSTE, PP PMSE, dengan UU PDP, untuk menguatkan pelindungan data pribadi dalam kegiatan *e-commerce*. Pemerintah juga perlu mengatur terkait bagaimana tanggung jawab pelaku usaha *e-commerce* saat terjadi kegagalan

[32] Pasal 72 ayat (1) Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
[33] Pasal 72 ayat (2) Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik

pelindungan data pribadi walaupun sudah menggunakan Sertifikat Keandalan Privasi. Hal ini menjadi penting, agar pelaku usaha *e-commerce* selaku pengendali data pribadi tidak lengah dan melepas tanggung jawabnya atas kegagalan yang terjadi.

DAFTAR PUSTAKA

Buku

Adi Sulistyo Nugroho, *E-Commerce Teori dan Implementasi* (Yogyakarta: Ekuilibria, 2016)

Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia* (Bandung: Refika Aditama, 2005).

Bagus Hanindyo Mantri, *Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce* (Semarang: Universitas Diponegoro, 2007).

Danrivanto Buhdijanto, *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity* (Bandung: Refika Aditama, 2023).

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law (Aspek Hukum Teknologi Informasi)* (Bandung: Refika Aditama, 2005)

Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003).

Endang Sri Wahyuni, *Aspek Hukum Sertifikasi & Keterkaitannya Dengan Perlindungan Konsumen* (Bandung: Citra Aditya Bakti, 2003)

Hendra Djaja, *Hukum Telematika* (Aspek-Aspek Hukum Informasi dan Transaksi Elektronik) (Malang: Surya Pena Gemilang, 2010).

OK. Saidin, *Aspek Hukum Hak Kekayaan Intelektual* (Jakarta: Raja Gravindo Persada, 2004).

Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Penerbit Kencana, 2007).

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

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

Soerjono Soekanto dan Sri Mahmudji, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat* (Jakarta: Raja Grafindo Persada, 2003).

Sugeng, *Hukum Telematika* (Jakarta: Prenadamedia Group, 2020).

Makalah/Artikel/Prosiding/Hasil Penelitian

Maichle Delpiero (et.al), "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," Padjadjaran Law Review, Vol. 9 No. 1 (2021).

Sugiharto, "Memanfaatkan E-Commerce Dengan Benar," Kementerian Keuangan, https://www.djkn.kemenkeu.go.id/artikel/baca/15814/Memanfaatkan-E-Commerce-Dengan-Benar.html (diakses 16 Juli 2023).

Yudha Hadian Nur dan Dwi Wahyuniarti Prabowo, "Penerapan Prinsip Tanggung Jawab Mutlak (Strict Liability) Dalam Rangka Perlindungan Konsumen," Buletin Ilmiah Litbang Perdagangan, Vol. 5 No. 2 (2011).

Internet

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

Bintoro Agung, "Kebijakan Safe Harbour, Tanggung Jawab E-Commerce 'Dibatasi'," CNN Indonesia https://www.cnnindonesia.com/teknologi/20170227142956-185-196481/kebijakan-safe-harbour-tanggung-jawab-e-commerce-dibatasi (diakses 18 Juli 2023).

Galuh Putri Riyanto, "Data 533 Juta Pengguna Facebook Bocor, Termasuk Indonesia," Kompas.com, https://tekno.kompas.com/read/2021/04/04/09330067/data-533-juta-pengguna-facebook-bocor-termasuk-indonesia?page=all (diakses 16 Juli 2023).

Meta Kebijakan Privasi, "Apa yang dimaksud Kebijakan Privasi dan apa yang dicakup di dalamnya?," Facebook https://id-id.facebook.com/privacy/policy/?entry_point=facebook_page_footer (diakses 17 Juli 2023).

Muhammad Amirulloh, "Kewajiban Sertifikat Keandalan dalam UU PDP: Bukti Pelindungan Data Pribadi dalam Sistem Elektronik," Universitas Padjadjaran https://blogs.unpad.ac.id/muhamadamirulloh/2022/12/29/kewajiban-sertifikat-keandalan-dalam-uu-pdp-bukti-pelindungan-data-pribadi-dalam-sistem-elektronik/ (diakses pada 16 Juli 2023).

Prof. Dr. Ahmad M Ramli, "Konten Medsos Tak Terkendali, "Safe Harbour" Digugat agar Tak Absolut," Kompas.com https://www.kompas.com/tren/read/2022/12/13/175705465/konten-medsos-tak-terkendali-safe-harbour-digugat-agar-tak-absolut?page=all (diakses 17 Juli 2023).

Tokopedia Pusat Edukasi Seller, "Penerapan Kebijakan Pelindungan Data Pembeli," Tokopedia https://seller.tokopedia.com/edu/kebijakan-data-pembeli/ (diakses 17 Juli 2023).

Peraturan Perundang-Undangan

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

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

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

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik