Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Table Of Content

Journal Cover 2
Author[s] Statement 3
Editorial Team 4
Article information 5
Check this article update (crossmark) 5
Check this article impact 5
Cite this article 5
Title page 6
Article Title 6
Author information 6
Abstract 6
Article content 7

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

ISSN (ONLINE) 2598 9928

SCAN ME

Website

INDONESIAN JOURNAL OF LAW AND ECONOMIC

PUBLISHED BY
UNIVERSITAS MUHAMMADIYAH SIDOARJO

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

EDITORIAL TEAM

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Assessing Legal Measures for Addressing Personal Data Misuse in Commercial Settings: A Critical Analysis

Tinjauan Hukum terhadap Mekanisme Penegakan Hukum atas Pelanggaran Penyalahgunaan Data Pribadi di Pasar

Salsabila Anissa, salsabilaa1525@gmail.com, (0)
Universitas Muhammadiyah Sidoarjo, Indonesia

Mochammad Tanzil Multazam, tanzilmultazam@umsida.ac.id, (1)
Universitas Muhammadiyah Sidoarjo, Indonesia

(1) Corresponding author

Abstract

This study delves into the legal framework governing personal data protection in Indonesia, focusing on mechanisms to safeguard information and penalize offenders. Employing a normative juridical and conceptual approach, statutory and conceptual analyses were conducted to identify pertinent legal provisions. Examination of primary and secondary legal sources was undertaken to scrutinize the enforcement of laws in cases of personal data abuse. Marketplaces, serving as pivotal platforms for transactions and data sharing, entail inherent risks to privacy and security. Users routinely disclose personal details, necessitating robust safeguards against misuse. The findings underscore the imperative of effective legal mechanisms to mitigate personal data abuse, ensuring enhanced privacy and security within Indonesian marketplaces.

Highlights :

- The study employs a normative juridical and conceptual approach to analyze the legal framework governing personal data protection in Indonesia.
- Marketplaces serve as crucial platforms for transactions and data sharing, necessitating effective mechanisms to safeguard personal information.
- Examination of primary and secondary legal sources reveals the need for robust enforcement measures to deter and penalize perpetrators of personal data abuse.

Keywords: Personal data protection, Indonesia, Marketplaces, Legal mechanisms, Data abuse

Published date: 2024-05-01 00:00:00

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Pendahuluan

Telah terjadi perubahan dalam aktivitas kehidupan manusia di berbagai bidang sebagai akibat dari perkembangan teknologi informasi yang sangat cepat dan secara langsung mempengaruhi munculnya kategori-kategori perbuatan hukum yang baru. Kerangka hukum dan regulasi pengembangan teknologi informasi harus didukung oleh pemerintah untuk memastikan bahwa teknologi informasi digunakan secara aman dan sesuai dengan nilai-nilai sosial budaya dan agama di Indonesia. Hal ini akan membantu mencegah penyalahgunaan teknologi dan mendorong perkembangannya.[1]

Kemunculan teknologi Internet memiliki dampak yang signifikan terhadap setiap aspek kehidupan manusia, termasuk aspek ekonomi, sosial, politik, dan bahkan pertahanan dan keamanan. Penggunaan media internet untuk teknologi informasi telah menciptakan peluang baru bagi model perusahaan yaitu, teknologi e-commerce adalah mekanisme komersial yang beroperasi secara elektronik dan berfokus pada transaksi bisnis online. Teknologi ini menawarkan kesempatan untuk membangun hubungan yang lebih intim dan personal dengan klien tanpa dibatasi oleh ruang dan waktu.[2]

Marketplace merupakan situs atau platfrom jual beli yang dilakukan secara online. Terdapat beberapa aplikasi Marketplace yang memiliki akses belanja online yang memudahkan pengguna platform Marketplace sebagai kebutuhan sehari-hari, karena pihak produsen menjual dan memasarkan barangnya secara langsung kepada pelanggan untuk transaksinya yang dilakukan secara online. Strategi bisnis ini memerlukan situs web yang tidak hanya membantu dalam pengiklanan produk, tetapi juga memudahkan pengecer online untuk melakukan transaksi keuangan secara online misalnya, Shopee, Blibli, Tokopedia, Bukalapak.

Beberapa pelanggan menggunakan pasar internet yang sudah ada sebagai sumber utama pembelian mereka. Pembeli dan penjual online mengkhawatirkan risiko yang terkait dengan berbagai keuntungan perdagangan online. Transaksi antara penjual dan pembeli dilakukan melalui internet (di dunia maya), yang sering kali sulit dilacak, dan bukan secara langsung, sehingga meningkatkan risiko. Kecenderungan bisnis tradisional menjadi online telah mengubah kebiasaan pasar, transaksi secara online antara penjual dan pembeli dengan melalui situs web atau toko online tanpa harus bertemu langsung. Hal tersebut memiliki kendala penerapan e-commerce, termasuk kelangkaan sumber daya manusia dan lemahnya keamanan e-commerce. Oleh karena itu, masalah keamanan, penipuan, dan ketidakpuasan pelanggan adalah tiga bahaya yang paling sering terjadi.

Pertumbuhan bisnis Marketplace yang menjadi hambatan adalah banyak aksi curang yang dilakukan oleh produsen Marketplace, yaitu penyalahgunaan data pribadi, di mana penggunaan data pribadi digital dapat diperdagangkan atau disalahgunakan (untuk tujuan selain pemberian atau penyerahan) tanpa sepengetahuan serta seizin pemilik data informasi, data juga dapat muncul bersama dengan tangkapan pribadi yang telah dicuri (diretas) oleh pihak ketiga. Ketika data pribadi digunakan dengan tidak semestinya, data tersebut dapat mengungkapkan kelemahan sistemik dan kurangnya pengawasan, sehingga membuka peluang penyalahgunaan dan membahayakan pemilik data. Menurut dasar uraian penelusuran tersebut, terdapat beberapa contoh dan masalah penyalahgunaan data dan informasi.[2]

Di Indonesia penyalahgunaan data pribadi timbul karena masih belum memahami bagaimana menjaga keamanan data mereka secara online. Sebagai hasilnya, mereka mungkin tidak cukup hati-hati dalam memasukkan informasi pribadi mereka ke dalam situs web atau aplikasi yang kurang terpercaya, saat mengunduh aplikasi, dan sebagainya yang tidak disadari dapat disalahgunakan bagi pelaku kejahatan data pribadi. Selain itu, sebagai efek dari pesatnya perkembangan ilmu pengetahuan dan teknologi, big data kini tersebar luas. Melihat big data sebagai potensi perbaikan untuk komputasi sehingga dapat menangani data yang besar dapat digunakan oleh sector swasta selain oleh pemerintah. Kesimpangsiuran yang disebabkan oleh pendaftaran data pribadi seperti nama dan alamat dalam kartu pribadi (KTP), nomor telepon, dan informasi pembayaran, contoh lainnya adalah riwayat aplikasi taksi online, yang mungkin merupakan penyalahgunaan data. Oleh karena itu perlu adanya aturan mengenai penyalahgunaan data pribadi.[4]

Berdasarkan hasil penelitian Sekaring Ayumeida Kusnadi & Andy Usmina Wijaya (2021) dengan judul Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. Penelitian ini bertujuan mempelajari lebih mendalam tentang perlindungan hukum di Indonesia untuk data privat sebagai hak atas pribadi, dan perbedaan perlindungan hukum data pribadi di walayah Asia termasuk sifat dan berbagai manifestasinya. Teknik analisis yang digunakan yuridis normatif (legal research) dengan pendekatan konseptual, mengevaluasi apakah seseorang bertindak sesuai dengan hukum (bukan hanya dengan peraturan hukum), prinsip-prinsip hukum, dan apakah peraturan hukum tersebut sesuai dengan perintah atau larangan yang sesuai dengan hukum. Studi ini menunjukkan bahwa warga negara memiliki hak konstitusional atas privasi, yang merupakan hakikat dari perlindungan hukum terhadap data pribadi. Saat ini belum ada ketentuan undang-undang atau peraturan di Indonesia yang menyediakan kerangka hukum untuk perlindungan data pribadi.[5]

Selanjutnya dari hasil penelitian Nurmalasari (2021) dengan judul Urgensi Pengesahan Rancangan Undang-undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. Teknik analisis yang digunakan yaitu yuridis normatif dengan menggunakan teknik-teknik untuk mengumpulkan data, seperti analisis deskriptif dan tinjauan literatur. Temuan-temuan tersebut menunjukkan bahwa RUU Perlindungan Data Pribadi memang membutuhkan

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

pengesahan yang cepat mengingat banyak faktor yang mendukungnya, seperti meningkatnya insiden pelanggaran data pribadi, kebutuhan untuk melindungi kebebasan warga negara, dan keinginan untuk memberikan ketentuan hukum kepada masyarakat.

Dan yang terakhir dari hasil penelitian Deanne Destriani Firmansyah Putri dan Muhammad Helmi Fahrozi (2021) dengan judul Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi. Tujuan dari penelitian ini adalah untuk mengetahui kasus kebocoran data dan menemukan solusi pada RUU Perlindungan Data Pribadi. Teknik analisis yang digunakan yaitu yuridis normatif dengan pendekatan perundang-undangan dan kasus. Studi ini menunjukkan berharganya RUU Perlindungan Data Pribadi untuk segera ditetapkan dan disahkan agar dapat mengadili para pelaku dan meminta pertanggungjawaban penyelenggara e-commerce. Tentu saja, masyarakat akan mendapatkan kepastian hukum untuk mengatasi masalah-masalah yang berkaitan dengan kebocoran data.

Berdasarkan penjelasan diatas, perbedaan antara penelitian ini dan penelitian sebelumnya yaitu penelitian ini untuk mengevaluasi sejauh mana peraturan mengenai perlindungan data pribadi telah berhasil dalam melindungi data pribadi individu dan memastikan penegakan hukum yang efektif terhadap penyalahgunaan data tersebut. Karena Tujuan utama artikel ini adalah untuk menganalisis aspek-aspek yuridis yang terkait dengan pelanggaran penyalahgunaan data pribadi dalam konteks pasar daring (marketplace). Menguraikan prinsip-prinsip yang harus diterapkan dalam kerangka UU Perlindungan Data Pribadi untuk marketplace. Prinsip-prinsip ini meliputi transparansi dalam pengumpulan dan penggunaan data pribadi, persetujuan yang jelas dari pengguna sebelum penggunaan data, dan keamanan yang memadai untuk melindungi data dari akses yang ilegal.

Terkait dengan isu tersebut, penting untuk dikaji karena untuk melindungi konsumen, menilai tanggung jawab platform, meningkatkan penindakan terhadap pelanggaran, meningkatkan kesadaran dan kepatuhan, serta membangun kepercayaan publik terhadap marketplace. Menekankan pentingnya mekanisme penegakan hukum dalam perlindungan data pribadi untuk melindungi data pribadi pengguna marketplace. Mekanisme ini harus memastikan bahwa marketplace memiliki kebijakan yang jelas tentang perlindungan data pribadi. Hal ini juga penting untuk melindungi privasi individu, membangun kepercayaan publik, dan memastikan bahwa entitas yang memproses data bertanggung jawab dan mematuhi peraturan yang berlaku. Mengatur dan memfasilitasi kemajuan teknologi dengan mengadopsi aturan yang sesuai merupakan salah satu usaha yang dilakukan untuk menurunkan kemungkinan dampak negatif yang diakibatkan oleh perubahan nilai ini.[3]

Analisis terhadap mekanisme penegakan hukum peraturan perlindungan data pribadi terhadap pelanggaran penyalahgunaan data pribadi sangat penting. Mengidentifikasi mekanisme penegakan hukum yang ada untuk menangani pelanggaran penyalahgunaan data pribadi di lingkup marketplace. Ini meliputi proses pengaduan, investigasi, dan tindakan penegakan hukum yang dapat diambil oleh pihak berwenang atau lembaga yang terlibat dalam menangani kasus-kasus tersebut. Untuk menjaga hak-hak dan privasi pengguna serta keamanan data pribadi mereka, sangat penting bahwa pelanggaran penyalahgunaan data pribadi di marketplace harus ditindak secara efektif oleh penegak hukum. Untuk menghentikan lebih banyak contoh eksploitasi data dan untuk menjaga kepercayaan publik terhadap ekosistem marketplace secara keseluruhan, tindakan penegakan hukum yang efektif juga penting.

Mengenai latar belakang dan uraian permasalahan diatas, maka yang menjadi permasalahan pokok adalah bagaimanakah mekanisme penegakan hukum yang berlaku di Indonesia terkait penyalahgunaan data pribadi konsumen Marketplace jika informasi pribadi mereka telah dicuri atau disalahgunakan serta apakah dampak hukum yang diterima oleh pelaku kejahatan data pribadi?

Metode

Metode yang digunakan dalam penelitian adalah Yuridis Normatif dengan pendekatan Perundang-undangan (statute approach) dan Pendekatan Konsep (conceptual approach) serta beberapa kasus yang menjadi acuan terkait penyalahgunaan data pribadi. Setelah itu, peneliti akan menganalisis dan menelaah sumber hukum primer dan sumber hukum sekunder untuk menemukan aturan hukum yang berlaku. Bahan hukum primer mengacu pada beberapa Undang-undang yang berlaku di Indonesia, antara lain:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Sistem Elektronik; 2. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik; 3. Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen; 4. *Peraturan Menteri Komunikasi dan Informatika* Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat; 5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan 6. *PeraturanPemerintah* (*PP*) Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Sedangkan sumber hukum sekunder meliputi buku- buku teks yang ditulis oleh ahli hukum dan jurnal-jurnal hukum.

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Hasil dan Pembahasan

1. Ruang Lingkup Teknologi Internet dan Definisi Cybercrime atas Perlindungan Data Pribadi

Prmenkominfo Republik Indonesia No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik mendefinisikan data pribadi sebagai data individu yang bersifat spesifik yang disimpan, dipelihara, dijaga keakuratannya, dan dilindungi kerahasiaannya. Antara pengendali data pribadi dan pengguna data, sesuai dengan Peraturan Menteri, terdapat hak dan kewajiban, dan system administrasi.[6]

Dalam hal proses akuisisi, pengumpulan, pemrosesan, analisis data, penyimpanan, penyajian, pengumuman, pengalihan, dan/atau pendistribusian, serta pemblokiran dan pemusnahan data, untuk mengamankan data pribadi, pihak ketiga memiliki hak dan tanggung jawab.[7] Untuk mencegah penggunaan data yang memicu kejahatan siber, data ini harus digunakan dan dikelola dengan hati-hati dan bertanggung jawab. Kejahatan dunia maya adalah segala aktivitas ilegal yang menggunakan komputer sebagai alat utama yang memanfaatkan teknologi komputer, khususnya internet. Berdasarkan tingkat kecanggihan perkembangan teknologi internet, kejahatan dunia maya didefinisikan sebagai tindakan ilegal yang memanfaatkan teknologi komputer.[8]

Tidak dapat dipungkiri bahwa penggunaan teknologi internet sangat membantu dalam menyelesaikan masalah-masalah yang menantang dengan sukses dan cepat. Namun, kecanggihan teknologi ini juga memiliki kemampuan untuk mendorong orang untuk berperilaku yang berlawanan dengan adat istiadat sosial yang berlaku. Dunia maya, dunia tanpa batas, atau realitas virtual (virtual reality), semuanya dimungkinkan oleh penggunaan teknologi internet, yang menciptakan peradaban global baru dan tidak lagi dibatasi oleh hubungan fisik negara yang sebelumnya dianggap sangat penting. Inilah yang dimaksud dengan Dunia Tanpa Batas.

Salah satu tren modern dalam perilaku kriminal kontemporer yang telah menarik perhatian dunia internasional adalah kejahatan dunia maya. Dalam arti sempit, kejahatan siber adalah kejahatan komputer yang ditargetkan pada sistem atau jaringan komputer, jika dilihat secara luas, kejahatan siber mencakup semua bentuk kejahatan baru yang ditargetkan pada komputer, jaringan komputer, dan penggunaannya, serta bentuk kejahatan konvensional yang saat ini dilakukan dengan bantuan perangkat (computer related crime). Dengan demikian, kejahatan cyber yang dilakukan antara lain:[9]

1. Dengan menggunakan prasarana dari sistem atau jaringan komputer (by means of a computer system or network); 2. Di dalam sistem atau jaringan komputer (in a computer system or network); 3. Melawan terhadap sistem atau jaringan komputer (against a computer system or network).

Menurut definisi ini, kejahatan dunia maya didefinisikan sebagai kejahatan komputer yang menargetkan sistem atau jaringan komputer dalam arti sempit, dan dalam arti luas, kejahatan ini mengacu pada jenis kejahatan baru yang menargetkan komputer, jaringan komputer, dan penggunanya, serta jenis kejahatan lama yang sekarang dilakukan dengan bantuan teknologi computer.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut "UU ITE") dan Peraturan Pemerintah Nomor 28 Tahun 2012 tentang Penyelenggaraan Sistem Elektronik, keduanya memuat ketentuan-ketentuan hukum yang secara umum mengatur mengenai kebijakan privasi pada sistem daring (online) yang terdapat pada Marketplace di Indonesia.

Sehingga Marketplace ini merupakan sistem e-commerce jadi yang memegang kendali lebih adalah sektor e-commerce utama pemerintah Indonesia yang merupakan Kementerian Komunikasi dan Informasi (Kemenkominfo), Kementerian Komunikasi dan Informatika mengelola program registrasi dan pengumpulan data bagi para pelaku di sektor bisnis e-commerce dengan menggunakan sejumlah prosedur profiling dan laporan berbasis data berdasarkan dua aturan regulasi tersebut. Hal ini bertujuan untuk melindungi pelanggan dari penipuan atas pelaku kejahatan atau yang dilakukan oleh orang perseorangan yang tidak bertanggung jawab.

Menurut tingkat keparahan bahaya yang disebabkan oleh pemrosesan data tanpa persetujuan, Petunjuk DP UE membuat perbedaan antara "data sensitif" dan "data tidak sensitif". Peraturan Perlindungan Data Umum (GDPR) Uni Eropa adalah undang-undang yang mengatur perlindungan data pribadi secara menyeluruh. GDPR mendefinisikan apa yang dimaksud dengan data pribadi, yang dapat mencakup nama, nomor identifikasi, informasi lokasi, pengenal online, atau satu atau lebih elemen tertentu yang berkaitan dengan ciri-ciri ekonomi, budaya, atau sosial seseorang. Hal ini juga mencakup pengidentifikasi pribadi seperti data yang tidak dapat diketahui yang dapat digunakan bersama dengan data lain untuk mengidentifikasi seseorang.

Di dalam situasi ini, negara berperan sebagai keadilan (justice) dan kewajaran (fairness) dengan bertindak sebagai "pihak di tengah" dan sebagai pihak yang memegang kendali atas kebijakan privasi (privacy policy) yang dibuat dan diakui oleh penyedia jasa/penjual layanan e-commerce dengan konsumen terkait data privasi berbasis online. Sehingga klausul kebijakan privasi yang normal, yang dalam situasi ini memiliki beberapa kekurangan, dapat diubah dengan segera dan hak-hak konsumen tidak dilanggar. Mekanisme kebijakan privasi dalam sistem online marketplace telah ditetapkan dalam berbagai peraturan hukum di dunia Internasional, terutama di negara-negara

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

yang telah memberlakukan undang-undang e-commerce di tingkat nasional, regional, dan internasional, termasuk negara-negara yang menjadi bagian dari Uni Eropa dan Amerika Serikat, serta telah mengembangkan peraturan e-commerce di tingkat tersebut (seperti EU Directive).

2. Mekanisme Pertanggungjawaban Pihak Penyelenggara yang Diberikan kepada Konsumen Marketplace

Seperti halnya pada sistem e-commerce saat ini sangat dibutuhkan bagi para penjual dan penyelenggara marketplace yang menyadari kemungkinan bahwa data privasi konsumen online memungkinkan penemuan dan penjualan produk secara sederhana sesuai dengan apa yang diinginkan secara tepat dan mudah, meskipun sudah jelas dalam hukum ekonomi klasik bahwa akan selalu ada penawaran (Demand) jika ada permintaan (Supply).[10]

Dalam upaya untuk memberikan kekuatan yang lebih besar kepada konsumen, sektor konsumen harus menyediakan ruang untuk penyelesaian konflik. Pengakuan terhadap kualitas unik dari kedudukan konsumen, khususnya adanya beda kepentingan yang mencolok antara dua pihak yang memiliki posisi negosiasi yang berbeda, ditunjukkan melalui upaya untuk memberdayakan atau memperkuat konsumen. Dalam Peraturan Mentri Kominfo PDPSE Penyelesaian perselisihan dibahas dalam bab terpisah yang dapat ditemukan dalam Pasal 29 hingga 33.

Sesuai dengan UU PDP Pasal 26 huruf b menyatakan bahwa pemilik data berhak mengadukan kepada Menteri atas kegagalan dalam melindungi data pribadi, Pasal 29 ayat (1) menjelaskan pengaduan atas kegagalan menjaga kerahasiaan data pribadi dapat diajukan kepada Menteri oleh pemilik data pribadi dan perusahaan yang memasok sistem elektronik[11].

Aturan yang berlaku pada Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen secara khusus mengatur penggunaan klausula baku dalam Pasal 18 ayat (1). Bagi pelaku usaha, pasal ini membatasi dan melarang penggunaan klausa baku. Sesuai dengan huruf a Pasal 18 UUPK, " Pelaku bisnis dilarang untuk atau menambahkan ketentuan standar pada setiap penawaran barang dan/atau jasa yang ditujukan untuk diperdagangkan". Jika bahasa baku mengatur pengalihan tanggung jawab pelaku usaha, maka hal tersebut harus dicantumkan dalam setiap dokumen dan/atau perjanjian. UUPK menyampaikan dalam ketentuan Pasal 18 ayat (3) menjelaskan bahwa "Setiap ketentuan pokok yang dibuat oleh pelaku usaha dalam suatu dokumen atau perjanjian sebagaimana dimaksud pada ayat (1) dianggap batal demi hukum."

Pada Pasal 8 PP PTSE, dibahas bagaimana PSE menyelenggarakan transaksi dengan menggunakan perangkat lunak berbasis digital. PSE harus menjamin keamanan dan ketergantungan kegiatan mereka berdasarkan Pasal 8 PP PTSE. Perlindungan data pribadi adalah topik utama dalam PP PTSE Pasal 14. Prinsip-prinsip perlindungan data pribadi harus diikuti oleh PSE ketika memproses data pribadi, Sesuai dengan Pasal 14 Ayat 1 Huruf E PP 71/2019, menurut huruf e pada kalimat pertama Pasal 14, pemrosesan data pribadi meliputi pengamanan terhadap kehilangan, penyalahgunaan, pengaksesan dan pengungkapan tanpa izin, pengubahan, dan pemusnahan. Pasal 14 ayat 5 PP PTSE menjabarkan tanggung jawab PSE untuk menginformasikan secara tertulis kepada pemilik data jika terjadinya pelanggaran keamanan data pribadi yang menjadi tanggung jawab PSE.

Menurut UU PDP Pasal 47, pengendali Data Pribadi bertanggung jawab untuk memproses Data Pribadi dan harus menunjukkan akuntabilitas dengan mengikuti aturan untuk melindungi Data Pribadi. Paragraf 2 Pasal 55 mewajibkan pengendali Data Pribadi untuk mematuhi definisi Perlindungan Data Pribadi dalam Undang-Undang saat mentransfer atau menerima Data Pribadi. Menurut kedua Pasal tersebut, Data Pribadi yang dikirim ke pengendali Data atau ditransfer kepada mereka yang dilindungi oleh Hukum dan Undang-Undang. Hal yang sama berlaku untuk perjanjian apa pun yang diperoleh pengendali Data tentang pengelolaan data.

Ada juga tujuan pengajuan pengaduan adalah untuk menyelesaikan perselisihan yang muncul melalui negosiasi atau bentuk penyelesaian konflik lainnya termuat dalam ayat 2 Pasal 29. Alasan-alasan untuk mengajukan pengaduan, seperti yang disebutkan dalam ayat (1), dijelaskan dalam Pasal 29 ayat (3). Kegiatan Menteri dalam menanggapi pengaduan dijelaskan dalam Pasal 29 ayat (4). Menurut ketentuan Pasal 31 huruf d, panel penyelesaian sengketa data pribadi harus merespons atau menyelidiki pengaduan yang dibuat oleh pengadu selambat-lambatnya 14 hari kerja setelah diterima, baik lengkap atau tidak.

Kewajiban ini muncul karena panel ini dibentuk sebagai tanggapan atas indikasi kegagalan dalam melindungi kerahasiaan data pribadi. Forum penyelesaian sengketa data pribadi harus mulai menangani penyelesaian pengaduan 14 hari setelah menerima pengaduan lengkap, sesuai dengan Pasal 31 huruf f. Hal ini diatur dalam Pasal 31 huruf G, yang mengatur bahwa pengaduan lengkap sebagaimana dijelaskan dalam Pasal 31 huruf f harus diselesaikan melalui musyawarah atau bentuk penyelesaian sengketa alternatif lainnya sesuai dengan peraturan perundangan yang berlaku.

Pasal ini menetapkan bahwa pengaduan harus didukung oleh data yang lengkap. Menurut Pasal 31 Huruf e, pengadu harus melengkapi pengaduan yang belum selesai dalam waktu 30 hari kerja setelah menerima pemberitahuan bahwa pengaduan tersebut belum selesai. Prosedur tindak lanjut yang dilakukan Menteri setelah menerima pengaduan tentang konflik yang melibatkan data pribadi dijelaskan dalam Pasal 30 ayat (1). Menteri akan memberikan kewenangan kepada Direktur Jenderal untuk menyelesaikan perselisihan terkait data pribadi sesuai dengan Pasal 30 ayat (Menurut Pasal 30 Ayat 2, Direktur Jenderal berwenang membentuk forum

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

penyelesaian sengketa data pribadi setelah menerima pendelegasian wewenang dari Menteri tentang penyelesaian sengketa data pribadi.

Setiap pemilik data yang menggunakan penyelenggara sistem elektronik dapat mengambil langkah hukum dengan mengajukan gugatan perdata terhadap kegagalan melindungi data pribadi apabila sengketa terkait kegagalan melindungi data pribadi tidak dapat diselesaikan melalui negosiasi atau alternatif lainnya. Gugatan hanya diajukan sebagai tindakan perdata dan mengikuti prosedur hukum. Pihak yang berwenang diharuskan untuk menyita data pribadi yang sesuai dengan masalah hukum ketika melaksanakan hukum oleh aparat penegak hukum yang bertindak sesuai dengan prinsip-prinsip hukum, menyita semua perangkat elektronik tidak diperlukan.

Berikut ini merupakan mekanisme pengajuan pengaduan penyelesaian sengketa dalam *Peraturan Menteri Komunikasi dan Informatika* Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat:

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

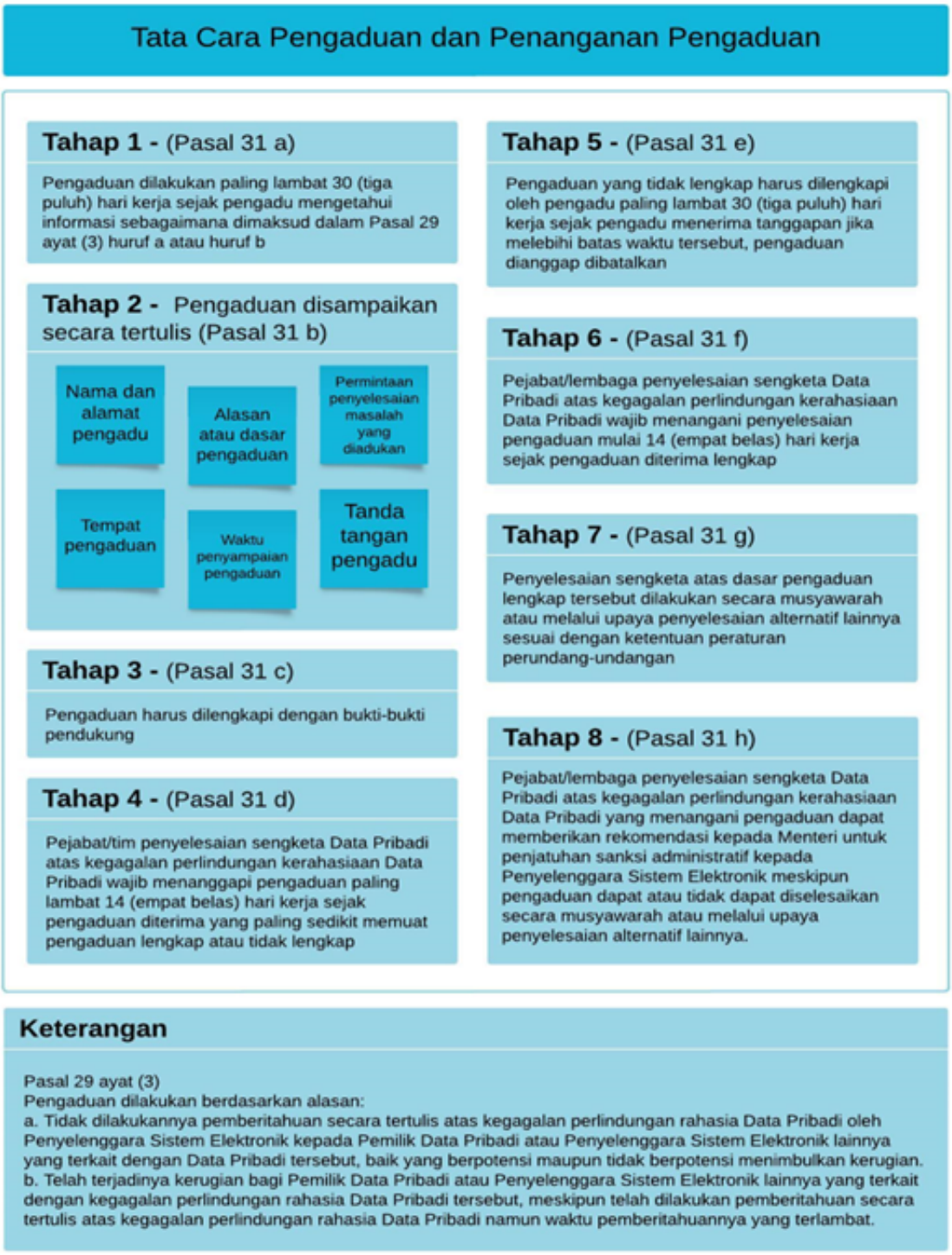

Figure 1. *Mekanisme Pengaduan Penyelesaian Sengketa dalam Sistem Elektronik*

3. Dampak Hukum yang Diterima oleh Pelaku Kejahatan atas Kasus Penyalahgunaan Data Pribadi

Salah satu kejahatan siber yang menyerang computer adalah serangan cyber di Tokopedia yang kronolginya adalah sebagai berikut. Garis waktu pembobolan akun Tokopedia dimulai pada hari Sabtu, 5 Februari, ketika peretas Whysodank memposting putaran pertama temuan peretasan di Forum Raid. Tanggal 20 Maret 2020 menandai tanggal peretasan. Kemudian, pada sore hari pukul 16:15 WIB, akun @underthebreach mencuit tentang peretasan tersebut dan menegaskan bahwa mereka menyediakan layanan untuk pengawasan dan pencegahan kebocoran untuk data yang berasal dari Israel. Menurut tangkapan layar yang diposting di media sosial, peretas masih perlu

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

mencari tahu metode untuk membuka kunci hash kata sandi. Untuk membuka kunci algoritme, peretas juga meminta bantuan dari peretas lain.[8]

Tangkapan layar akun pembocor informasi berikut ini menunjukkan beberapa akun pengguna yang dapat dibuat di situs web. Situs web tersebut menampilkan nama, alamat email, dan nomor telepon pengguna. Meskipun peretas mengklaim ada lebih banyak pengguna yang terpengaruh, serangan tersebut sebanyak 15 juta orang terkena dampaknya pada bulan Maret 2020. Situs data (yang diretas) berisi email, kata sandi, dan nama. Keesokan harinya, Whysodank mengungkapkan di forum darkweb bernama EmpireMarket bahwa mereka telah menjual data dari 91 juta pengguna Tokopedia. Data kata sandi akun Tokopedia masih terenkripsi, tetapi menurut pakar keamanan siber Pratama Persadha, Hanya masalah waktu saja sebelum seseorang dapat mendekripsinya.

Oleh karena itu, para penjahat bertujuan untuk melakukan pembagian gratis pada beberapa akun untuk mengarang cerita tentang siapa yang memecahkan kode kata sandi tersebut. Pratama mengklaim bahwa meskipun kata sandi masih dibuat secara acak, nformasi lainnya sekarang dalam bentuk biasa atau terbuka. Hal ini menyiratkan bahwa semua peretas dapat menggunakan informasi tersebut untuk melakukan penipuan dan membajak akun online. Misalnya, memposting tautan phishing atau melakukan upaya rekayasa sosial lainnya, Tokopedia harus segera memperbarui dan memperingatkan semua pengguna. Pengambilalihan akun merupakan salah satu hal yang akan terjadi jika pelakunya kemudian berhasil membuka kata sandi. Karena menggunakan kata sandi yang sama di berbagai platform adalah hal yang umum, pelaku kejahatan akan mencoba secara acak untuk menguasai akun media sosial dan marketplace lainnya. Pratama menekankan bahwa pengguna Tokopedia memiliki opsi untuk mengubah kata sandi dan mengaktifkan OTP (one-time password) melalui SMS. Setelah itu, ubahlah kata sandi untuk semua akun media sosial dan toko online selain Tokopedia.[12]

Serangan Tokopedia dapat meluas ke akun media sosial dan platform lainnya jika email dan password yang digunakan sama. Administrator akun media sosial resmi dan institusi harus segera mengamankan akun mereka sebagai tindakan pencegahan, tidak ada informasi kartu kredit atau debit yang disebarkan ketika data sampel diperoleh dari forum oleh pelaku. Kami berharap informasi kartu tersebut tidak menjadi salah satu yang berhasil dibobol, mengingat data pengguna Tokopedia dicuri dan dijual, maka kejadian ini merupakan kesalahan Tokopedia. Tokopedia perlu berulang kali menggunakan semua media yang dimilikinya untuk menyebarkan informasi tentang apa yang perlu dilakukan oleh para penggunanya, seperti mengganti kata sandi akun dan mengaktifkan OTP, hingga semua pengguna menyadari adanya pembobolan tersebut dan mau mengganti kata sandi mereka.

Kemudian mengenai kasus mengenai kebocoran data pengguna Bukalapak, Jumlah pengguna Bukalapak yang datanya ditransfer meningkat menjadi 12,9 juta. Diyakini bahwa informasi dalam pelanggaran ini berasal dari bulan Maret 2019. Sampel data yang disediakan oleh peretas, termasuk yang ada di raidforum, menunjukkan bahwa kata sandi akun pengguna sebenarnya di-hash menggunakan enkripsi satu arah. Data yang dapat digunakan untuk mengidentifikasi orang-orang tertentu juga disertakan. Pertanggungjawaban pidana peretasan (hacking) di dasarkan pada ketentuan pasal 30 UU ITE. Menurut Pasal 30 UU ITE, mengakses komputer atau sistem elektronik korban tanpa izin dapat dihukum, dan metode apa pun, termasuk peretasan, dapat digunakan untuk melakukan kejahatan tersebut.

Vendor layanan web hosting tidak bertanggung jawab secara pidana atas peretasan situs web. Pemilik penyedia layanan web hosting tidak dapat menghindari tuntutan pidana meskipun layanan tersebut hanyalah penyedia media jika digunakan secara eksklusif untuk membantu aktivitas ilegal. Dengan nada yang sama, operator gedung apartemen tidak dapat dimintai pertanggungjawaban jika sekelompok perampok masuk ke unit pemilik apartemen. Di Indonesia, istilah "pemidanaan" seharusnya digunakan untuk menggambarkan strategi normatif yang menghukum para pelaku kejahatan untuk memberikan dampak jera. Sesuai dengan kebutuhan masyarakat akan hukum dan keadilan, penegakan hukum harus berjalan sesuai dengan visi dan misinya di semua tingkatan, mulai dari tingkat penyidik, penuntut umum, hingga pengadilan.[13]

Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yaitu Pasal 32 dan Pasal 48 ayat 1 dan ayat 2, maka analisis yang diperoleh dari kasus kejahatan siber hacker merupakan salah satu perbuatan melawan hukum. Dengan adanya pengaturan khusus dalam UU ITE mengenai tindak pidana yang melibatkan media elektronik, maka ketentuan dalam KUHP tidak berlaku lagi, sesuai dengan pepatah hukum lex specialis derogate legi generali, yang menyatakan, "Ketentuan khusus berlaku jika suatu perbuatan diatur oleh ketentuan pidana umum dan ketentuan pidana khusus." Hal ini seharusnya menjadi peringatan yang jelas bagi setiap penyedia layanan internet yang operasinya melibatkan penggunaan data publik secara luas.

Dari adanya penyalahgunaan data pribadi tersebut, maka jelas bahwa adanya kecacatan sistemik dan pengawasan yang kurang memungkinkan terjadinya eksploitasi data pribadi yang berakibat pada kerugian pemilik data. Penyalahgunaan, pencurian, dan penjualan data pribadi merupakan praktik teknologi informasi ilegal yang juga dapat dikategorikan sebagai pelanggaran hak asasi manusia karena data pribadi merupakan salah satu komponen hak asasi manusia yang harus dilindungi. Atas dasar perbuatan tersebut pelaku mendapatkan sanksi atau hukuman yang berdasarkan dengan ketentuan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE.

Jaksa mendasarkan tuduhan dan tuntutannya terhadap pelaku pada pasal tersebut. Kantor kejaksaan

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

mengeluarkan surat P21 untuk memulai proses membawa mereka yang bertanggung jawab atas kejahatan siber ke pengadilan ketika penyidik mengirimkan materi ke jaksa dan dianggap lengkap. Setelah tersangka dan barang bukti diserahkan ke kejaksaan, proses penuntutan dimulai. Pengadilan kemudian akan menentukan hari persidangan setelah menerima bukti dan surat dakwaan dari kejaksaan.

Adanya penjelasan tambahan dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengubah Peraturan Pemerintah No. 82 Tahun 2012, adalah peraturan baru. Namun, ketentuan Pasal 3 Ayat 1 PP PTSE tidak berdasar dalam keadaan kahar atau kecerobohan pengguna yang dapat dibuktikan terjadi. Sehingga PSE harus menggunakan sistem elektronik secara aman, andal, dan bertanggung jawab. Namun, dalam hal terjadi keadaan kahar dan/atau terbukti adanya kealpaan pengguna sistem elektronik.

UU ITE dan peraturan yang menyertainya membuat Marketplace bertanggung jawab atas hilangnya data konsumen, dan mereka telah mengambil sejumlah langkah untuk mengamankan sistem elektronik mereka dan menggunakan manajemen risiko sesuai dengan hukum. Pelanggan Marketplace dapat menuntut pertanggungjawaban Marketplace jika mereka yakin bahwa mereka telah kehilangan uang sebagai akibat dari situasi ini. Hukuman administratif, seperti peringatan tertulis, denda administratif, penangguhan sementara dan penghentian akses, dan bahkan tindakan hukum, dapat digunakan untuk meminta pertanggungjawaban orang atas tindakan mereka.

Terkait dengan hal tersebut bahwa sanksi administratif sebagaimana tercantum pada Pasal 80 ayat (2) PP PMSE yang telah diberikan oleh Menteri sesuai ketentuan perundang-undangan. Yang menjelaskan bahwa peringatan tertulis, penempatan daftar prioritas pengawasan, blacklist, pelarangan sementara layanan PPMSE domestik dan/atau internasional oleh instansi terkait, dan/atau pembatalan izin usaha adalah contoh-contoh sanksi administratif yang diatur.

Sedangkan penjelasan mengenai penjatuhan sanksi administratif yang tidak dapat menghilangkan tanggung jawab pidana dan perdata. UU ITE menguraikan hukuman pidana untuk pencurian informasi pribadi. Pasal 46 hingga Pasal 50, serta Pasal 61 dan 64 RUU PDP, mengatur pertanggungjawaban pidana. Menurut Pasal 65 RUU PDP, hukuman tambahan juga dapat diterapkan, termasuk pembayaran ganti rugi dan perampasan aset dan/atau pendapatan yang diperoleh sebagai hasil dari aktivitas ilegal. RUU PDP kemudian menjelaskan tentang pertanggungjawaban korporasi dalam Pasal 66.

Selain itu, pertanggungjawaban korporasi diatur dalam Sesuai dengan ayat 4 Pasal 52 UU ITE, korporasi yang melakukan tindak pidana dapat dikenai pidana pokok ditambah dengan pidana tambahan dua pertiga. Menurut ketentuan Pasal 26 Ayat (2) UU No. 19 Tahun 2016, setiap korban yang hak privasinya dilanggar dapat mengajukan gugatan perdata atas dasar hukum. Berdasarkan Menurut Kitab Undang-Undang Hukum Perdata Pasal 1365, bahwa setiap orang melakukan tindakan ilegal yang merugikan pihak ketiga, mereka bertanggung jawab untuk mengganti kerugian tersebut, maka pelanggaran terhadap perlindungan kerahasiaan data pribadi pengguna marketplace dapat dituntut sebagai tindak pidana.

Pasal 28 huruf c Permenkominfo PDPSE mengatur lebih lanjut mengenai prosedur notifikasi jika terjadi pelanggaran perlindungan data pribadi serta tindakan apabila terjadinya kegagalan. Menurut Pasal 28 huruf c, PSE harus memberikan pemberitahuan tertulis mengenai pelanggaran perlindungan data pribadi kepada pemilik data, dengan persyaratan pemberitahuan sebagai berikut:

(a) Pemberitahuan harus menyertakan penyebab atau alasan kegagalan mengamankan informasi pribadi yang sensitif; (b) Pemberitahuan dapat dilakukan secara elektronik jika persetujuan pemilik data pribadi, hal tersebut dinyatakan pada saat melakukan hasil dan pengumpulan data pribadi; (c) Pemberitahuan dipastikan telah diterima dan diverifikasi oleh pemilik data pribadi jika mengalami kegagalan sehingga menyebabkan kerugian pada orang yang bersangkutan; dan (d) Pemberitahuan tertulis harus dikirim ke subjek data selambat-lambatnya 14 (empat belas) hari setelah kegagalan ditemukan.

Serta telah dijelaskan pada Undang-undang 27 Tahun 2022 tentang Perlindungan Data Pribadi bahwa adanya sanksi Ketika seseorang melakukan kejahatan tidak penyalahgunaan data pribadi yang terdapat pada Pasal 65 ayat (1) bahwa melanggar hukum bagi siapa pun untuk mengakses atau mengumpulkan data pribadi tanpa izin dengan maksud untuk menggunakannya demi keuntungan mereka sendiri atau orang lain, karena hal tersebut dapat membahayakan subjek data pribadi. (2) bahwa melanggar hukum bagi siapa pun untuk menunjukkan Data Pribadi yang bukan miliknya secara tidak patut. (3) Menggunakan data pribadi orang lain tanpa izin merupakan pelanggaran hukum. Menggunakan informasi pribadi seseorang untuk mendapatkan keuntungan finansial secara tegas dilarang dalam artikel ini dan diakui sebagai tindak pidana.

Karena ketidaktelitian korban (masyarakat) dalam menjalankan tugas sehari-hari, penyalahgunaan data pribadi bisa saja terjadi tanpa disengaja. Misalnya, ketika membeli kartu perdana dan kemudian meminta petugas konter untuk meregistrasikannya, mengunduh aplikasi, termasuk Marketplace, mencantumkan data pribadi dalam formulir, dan contoh-contoh lain di mana petugas konter berpotensi menyalahgunakan informasi tersebut dan dampak bagi pemilik data yaitu mengalami kerugian. Meskipun aturan yang secara khusus mengatur data pribadi masih dalam tahap pengembangan, metode hukuman yang ada saat ini masih belum ideal.

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

Undang-Undang Perlindungan Konsumen No. 8 Tahun 1999 (UUPK) membahas sejumlah isu penting, termasuk hak konsumen untuk menerima layanan yang maksimal, hak untuk mendapatkan kompensasi, dan hak konsumen untuk mengajukan keluhan. Peraturan-peraturan ini dapat digunakan untuk memeriksa konsep perlindungan data pribadi di bawah hukum Indonesia. Pengaturan mengenai tanggung jawab dan ganti rugi merupakan aspek lain dari UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

UUPK maupun UU ITE tidak secara eksplisit mengurus tanggung jawab pelaku usaha terhadap konsumen dalam transaksi digital. UU ITE menjelaskan kegiatan transaksi digital tanpa menyebutkan e-commerce, sedangkan UUPK secara eksklusif mengacu pada kegiatan jual beli tradisional. Ketika membeli dan menjual produk secara online, konsumen mungkin merasa sulit untuk meminta pertanggungjawaban pelaku usaha karena kelemahan ini. Ketika mereka merasa diperlakukan tidak adil oleh pelaku usaha, konsumen akan mengambil tindakan. Undang-Undang Informasi dan Transaksi Elektronik dapat digunakan sebagai landasan hukum untuk menyelesaikan masalah dengan e-commerce dalam hal kerugian konsumen.[14]

Pelanggan atau calon pelanggan dapat memberikan informasi pribadi kepada pelaku usaha atau penyelenggara sistem elektronik secara offline maupun online. Namun, karena data pribadi yang terhubung dapat diperjualbelikan, dicuri, atau disalahgunakan tanpa sepengetahuan atau persetujuan pemiliknya, maka ada kemungkinan pihak ketiga dapat mengakses data pribadi yang terhubung dan menggunakannya untuk kepentingan mereka atau terjadinya pencurian data (hack). Memanfaatkan teknologi dan informasi dapat membantu di berbagai bidang, termasuk pendidikan, ekonomi, dan bidang lain yang dapat diakses dengan mudah, memungkinkan penerimaan miliaran atau bahkan triliunan informasi dengan cepat. [15]

Dalam bidang pekerjaan, penanganan data dalam jumlah besar dapat dilakukan dengan benar, cepat, efektif, dan efisien, sekaligus meminimalkan kesalahan. Promosi dan peluang di sektor ekonomi dilakukan dengan cepat, tanpa memandang lokasi atau wilayah, dan mempengaruhi setiap lapisan masyarakat dalam skala nasional dan internasional dapat memperoleh manfaat dari kapasitas untuk meningkatkan kesejahteraan masyarakat dengan cepat, terlepas dari lokasi atau wilayahnya. Namun, seiring dengan kemajuan informasi dan teknologi, hal tersebut juga membawa masalah yang dapat merugikan masyarakat, termasuk penyalahgunaan data, pencurian identitas, penjualan data pribadi, penipuan, dan masalah lainnya.

Simpulan

Perlindungan data pribadi menjadi semakin penting dalam era digital, terutama di lingkungan marketplace. Perdagangan elektronik telah berkembang pesat dan menyediakan kesempatan bagi banyak pengguna untuk berinteraksi dan bertransaksi dalam skala global. Namun, di tengah kemudahan ini, ada risiko besar terhadap privasi dan keamanan data pribadi pengguna. Oleh karena itu, konsumen dapat melaporkan dugaan penyalahgunaan data pribadi mereka kepada penyedia marketplace tempat data mereka terdaftar. Setiap platform marketplace biasanya memiliki mekanisme pelaporan atau pengaduan yang dapat diakses oleh pengguna. Jika terjadi dugaan pelanggaran privasi data oleh marketplace atau pihak ketiga, konsumen dapat mengajukan pengaduan ke BPDP sebagai otoritas yang bertanggung jawab mengawasi perlindungan data pribadi di Indonesia. Konsumen yang dirugikan oleh penyalahgunaan data pribadi juga dapat mengajukan gugatan perdata melalui jalur hukum, seperti pengadilan, untuk meminta ganti rugi atas kerugian yang diderita akibat dari pelanggaran privasi.

References

1. B. Sugiswati, "Aspek Hukum Telematika terhadap Kemajuan Teknologi di Era Informasi," vol. XVI, no. 1, Jan. 2011.
2. E. A. Pratama, "Optimalisasi Cyberlaw Untuk Penanganan Cybercrime Pada Ecommerce," Purwokerto, Indonesia, 2013.
3. L. Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia," Banda Aceh, Indonesia, vol. 20, p. 377, 2018.
4. S. M. T. Situmeang, "Penyalahgunaan Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber," in SASI, vol. 27, no. 1, pp. 38, Mar. 2021, doi: 10.47268/sasi.v27i1.394.
5. M. Edmon, "Kompilasi Hukum Telematika," 1st ed. Jakarta, Indonesia: PT RajaGrafindo Persada, 2003, pp. 510–511.
6. D. M. A. Mansur and E. Gultom, "Cyber law: aspek hukum teknologi informasi," 1st ed. Bandung, Indonesia: Refika Aditama, 2005.
7. S. Partodihardjo and Indonesia, Eds., "Tanya jawab sekitar Undang-Undang no. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik: dilengkapi dalam bentuk pointers," Jakarta, Indonesia: Gramedia Pustaka Utama, 2009, p. 73.
8. A. M. Ramli, "Cyber law & HAKI dalam sistem hukum Indonesia," 1st ed. Bandung, Indonesia: Refika Aditama, 2004.
9. L. Endah, "Tinjauan Yuridis Kartu Kredit di Indonesia," Surabaya, Indonesia: Universitas Narotama Surabaya, 2012.
10. Nurjiha, "E-Commerce Perspektif Generasi Milenial pada Media Sosial Facebook," Sep. 2022.

Vol 19 No 2 (2024): May
DOI: https://doi.org/10.21070/ijler.v19i2.1012
Article type: (Private Law)

11. Sy. H. Azizurrahman, "Pembaharuan Kebijakan Penegakan Hukum Pidana, Masalah Masalah Hukum Jilid 41 No. 2," Fakultas Hukum Universitas Diponegoro, Apr. 2012, p. 16.
12. A. Christie et al., "Lembaga Riset Ungkap Hacker Pembobol Data Pengguna Tokopedia," May 2020.
13. A. W. Laksana, "Tinjauan Hukum Pemidanaan Terhadap Pelaku Penyalahguna Narkotika Dengan Sistem Rehabilitasi," 2016, p. 75.
14. K. D. R. Natha, "Perlindungan Hukum atas Kebocoran Data Pribadi pada Perdagangan Elektronik Lokapasar (Marketplace)," Mar. 2022, doi: https://doi.org/10.22225/jph.3.1.4674.143-148.
15. W. A. Dairobbi, "Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi dalam Layanan Transportasi Berbasis Aplikasi Online," Aug. 2020.

ISSN 2598 9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo