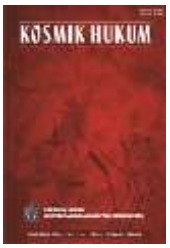

# Kosmik Hukum

**Fakultas Hukum**
**Universitas Muhammadiyah Purwokerto**
**Vol. 22 No. 1 (2022)**



# Urgensi Pembaharuan Hukum mengenai Perlindungan Data Pribadi E-Commerce di Indonesia

**Bram Freedrik Sangojoyo**✉, **Aurelius Kevin, David Brilian Sunlaydi**
Magister Ilmu Hukum Fakultas Hukum Universitas Airlangga Surabaya, Indonesia

E-mail Korespondensi: bramfreedrik53@gmail.com

**Article Process**

**Submitted:**
4-11-2021

**Reviewed:**
20-12-2021

**Revised:**
4-1-2022

**Accepted:**
12-1-2022

**Published:**
31-1-2022

***Abstract***

*E-commerce in Indonesia is increasing, especially since the Covid-19 pandemic. Electronic transactions run effectively and efficiently because there are facilities in the e-commerce platform that provide a variety of products to help people meet their dailyneeds. The use of e-commerce platforms requires all users to register first using their name, phone number, e-mail and some other personal data before they can take advantage of the facility. Unfortunately, there are cases of data leaks that are massively done by taking data contained in the e-commerce platform and sold freely on illegal websites. One of the factors that influence the occurrence of data leaks is the absence of comprehensive rules governing the protection of personal data in Indonesia. The purpose of this study is to analyze the form of legal protection of personal data of e-commerce users in Indonesia and see the comparison of personal data protection laws in Indonesia with those in Malaysia and Singapore. The results explained that there are regulations in the form of ministerial regulations governing the protection of personal data electronically, but the rules do not provide data protection expressly and far behind the rules in some ASEAN countries such as Malaysia and Singapore, so there needs to be a renewal of the law regarding data protection in Indonesia by issuing regulations at the level of laws as regulated and implemented. n in the Personal Data Protection Act of Malaysia and Singapore which also conform to EU GDPR rules. It aims to tighten the security of data managed by private parties and impose strict sanctions on anyone who accesses, collects, and transports data in an unauthorized or unlawful manner.*

***Keywords:*** *Personal Data Protection, e-Commerce, Legal Renewal.*

**Abstrak**

Perdagangan elektronik (e-commerce) di Indonesia kian hari kian meningkat terutama sejak adanya pandemi covid-19. Transaksi elektronik berjalan dengan efektif dan efesien karena terdapat fasilitas dalam platform e-commerce yang menyediakan berbagai macam produk guna membantu masyarakat memenuhi kebutuhan hidupnya. Pemakaian platform e-commerce mengharuskan semua penggunanya melakukan pendaftaran terlebih dahulu dengan menggunakan nama, nomor telepon, e-mail dan beberapa data pribadi lain sebelum dapat memanfaatkan fasilitas tersebut. Sayangnya, terdapat kasus kebocoran data yang secara masif dilakukan dengan mengambil data-data yang ada di dalam platform e-commerce tersebut dan dijual secara bebas pada website ilegal. Salah satu Faktor yang mempengaruhi terjadinya kebocoran data adalah belum adanya sarana beserta aturan yang secara komprehensif mengatur tentang perlindungan data pribadi di Indonesia. Tujuan penelitian ini adalah untuk mengalisis terkait bentuk perlindungan hukum data pribadi pengguna e-commerce di Indonesia dan melihat perbandingan hukum perlindungan data pribadi di Indonesia dengan yang ada di Malaysia dan Singapura. Penelitian ini menggunakan metode penelitian yuridis normatif. Hasil penelitian menerangkan bahwa terdapat regulasi berupa peraturan menteri yang mengatur tentang perlindungan data pribadi secara elektronik, akan tetapi aturan tersebut tidak memberikan perlindungan data secara tegas dan jauh tertinggal dengan aturan-aturan di beberapa negara ASEAN seperti Malaysia dan Singapura, sehingga perlu adanya pembaharuan hukum mengenai perlindungan data yang ada di Indonesia dengan menerbitkan regulasi setingkat Undang-Undang seperti yang diatur dan diimplementasikan di UU PDP Malaysia dan Singapura yang juga menyesuaikan dengan aturan EU GDPR. Hal tersebut bertujuan untuk memperketat keamanan data yang dikelola oleh pihak swasta dan memberi sanksi tegas bagi siapa saja yang mengakses, mengumpulkan, dan menstransfer data dengan cara tidak sah atau melawan hukum.

**Kata kunci**: Perlindungan Data Pribadi, e-Commerce, Pembaharuan Hukum.

**Kosmik Hukum Vol.** 22 No. 1 (2022): 27-39
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v22i1.12154

# I. Pendahuluan

Perkembangan dunia teknologi informasi saat ini telah merambah ke seluruh aspek bidang, baik pemerintahan, pendidikan, ekonomi dan lain-lain. Pada bidang ekonomi, teknologi informasi telah berhasil menggeser kebiasaan masyarakat dalam bertransaksi konvensional menjadi berbasis digital. Inovasi digital dibidang bisnis terus dikembangkan, diperbaiki dan diperbaharui untuk menambah minat masyarakat dalam bertransaksi lebih mudah melalui transaksi elektronik yaitu *e-commerce*. *E-commerce* ialah proses aktivitas perdagangan seperti pembelian, penjualan dan pemasaran barang dan jasa dengan memanfaatkan teknologi elektronik yang pada umumnya menghubungkan perusahaan, konsumen dan masyarakat dalam transaksi tersebut. [1]

Puncak tingginya transaksi *e-commerce* di Indonesia terjadi di tengah masa pandemi covid-19. Beberapa regulasi yang diterbitkan pemerintah guna menekan penyebaran virus tersebut baik dalam lingkup skala kecil hingga skala besar mengakibatkan masyarakat mengurangi mobilitas di luar rumah dan beralih pada platform *e-commerce* untuk memenuhi kebutuhan sehari-hari. Kondisi tersebut telah meningkatkan jumlah pengguna *e-commerce* di Indonesia. Septriana Tangkary selaku Direktur Pemberdayaan Informatika menerangkan bahwa pertumbuhan nilai *e-commerce* di Indonesia mencapai angka tertinggi di dunia[2]. Tingginya pengguna *e-commerce* tersebut didukung oleh persyaratan pendaftaran yang mudah pada *marketplace*, yaitu cukup mendaftar menggunakan Kartu Tanda Penduduk (KTP), Nomor telepon, *e-mail*[3], artinya untuk memakai layanan (*service*) dalam *e-commerce* tersebut harus memasukkan data pribadi para pengguna. Situasi tersebut berpengaruh pada rentannya serangan siber dan keamanan data masyarakat.[4]

Kebocoran data pribadi *(disclosure of data)* telah dialami beberapa pengguna *e-commerce* selama 2 (dua) *tahun* terakhir yaitu Tokopedia, Kreditplus, Reddoorz[5], Lazada, Bhinneka, Bukalapak[6] . Terdapat 91 (sembilan puluh satu) juta dan 7 (tujuh) juta data *merchant* yang telah berhasil di retas[7]. Pada tahun sebelumnya Tokopedia juga telah mengumumkan diretasnya kurang lebih 91 (sembilan puluh satu) juta akun di platformnya, yang berarti hampir keseluruhan akun pada platform Tokopedia berhasil dicuri data-data pribadinya oleh oknum dengan *nickname "why so dank"*[8].

Kasus yang sama juga di alami oleh Perusahaan *e-commerce* Lazada, yang menginformasikan bahwa terdapat 1,1 (satu koma satu) juta akun pengguna/konsumen Lazada telah diretas. *E-commerce* Bhinneka juga mengalami kasus yang sama yaitu diretasnya 1,2 (satu koma dua) juta data penggunanya. Perusahaan *e-commerce* Bukalapak juga mengalami kebobolan sebanyak 13 (tiga belas) juta data pengguna berhasil diretas oleh oknum tidak bertanggung jawab. Data-data yang telah diretas oleh pelaku pada umumnya berupa data pribadi sesuai yang tercantum dalam KTP, nomor telepon, dan *e-mail*, selanjutnya data-data tersebut dijual oleh pelaku ke *website* ilegal. Serangan pencurian data-data pribadi masih terus dilakukan secara masif, hal tersebut dapat dilihat dari data Badan Siber dan Sandi Negara (BSSN) yang

---

1 Mohammad Aldrin Akbar dan Sitti Nur Alam, *E-Commerce Dasar Teori dalam Bisnis Digital*, (Medan: Yayasan Kita Menulis, 2020), hlm. 1

2 Kominfo, Kemkominfo: Pertumbuhan e-Commerce Indonesia Capai 78 Persen, dari laman https://kominfo.go.id/content/detail/16770/kemkominfo-pertumbuhan-e-commerce-indonesiacapai-78-persen/0/sorotan_media; diakses pada 24 Oktober 2021

3 *Ibid*.

4 Ratnadi Hendra W., "Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19", *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, Vol. 22 No. 2 (2020): hlm. 142.

5 Sulasi Rongiyati, "Urgensi Sinergitas Pengaturan Pelindungan Data Pribadi dan Keamanan Siber Nasional", *Jurnal Info Singkat Bidang Hukum Pusat Penelitian Badan Keahlian DPR RI,* Vol. XIII No. 11/I/Puslit/Juni/2021, hlm. 1-2.

6 Imantoko Kurniadi, Lazada Singapura Akui Kebobolan 1,1 Juta Data Pribadi Penggunanya, laman dari https://selular.id/2020/11/lazada-singapura-akui-kebobolan-11-juta-data-pribadi-penggunanya/; diakses tanggal 24 Oktober 2021

7 Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen", *2nd National Conference on Law Studies: Legal Development Towards a Digital Society Era, 2020,* hlm. 46.

8 *Ibid*.

mengumumkan terdapat 88,4 (delapan puluh delapan koma empat) juta serangan siber yang dilancarkan sejak Januari sampai dengan April 2020. [9] Upaya Peretasan tentu hingga saat ini masih terus dilakukan oleh oknum-oknum yang tidak bertanggung jawab demi keuntungan pribadinya.

Data Pribadi merupakan hak privasi yang secara konstitusional dijamin perlindungannya. Jaminan tersebut termaktub dalam pasal 28G ayat (1) Undang-Undang Dasar Tahun 1945 (UUD 1945) yang menyatakan:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"

Jaminan perlindungan hukum data pribadi di Indonesia masih sangat minim dan masih belum komprehensif. Hal tersebut disebabkan aturan mengenai perlindungan data pribadi terdapat diberbagai peraturan perundangan-undangan dan sifatnya masih universal (umum). Menurut Pendapat Waluyo terdapat kurang lebih 14 (empat belas) Undang-Undang di Indonesia yang mempunyai pasal-pasal tentang pengaturan data pribadi, akan tetapi hingga saat ini belum ada payung hukum yang komprehensif membahas perlindungan data pribadi di Indonesia. Hal ini menyebabkan aturan tersebut masih bersifat sektoral serta menimbulkan berbagai pemahaman yang berbeda berkaitan dengan data pribadi. [10]

Payung hukum yang kurang spesifik mengenai pengaturan data pribadi di Indonesia, pada akhirnya tidak memberikan kepastian hukum bagi masyarakat untuk mendapatkan perlindungan hukum apabila terdapat kebocoran atau penyalahgunaan data pribadi penggguna situs atau platform *e-commerce.* Guna menjamin hal tersebut, maka perlu adanya peran negara maupun swasta serta regulasi hukum setingkat undang-undang agar perlindungan dapat diberikan secara pasti dan tegas.

Penelitian ini merujuk pada penelitian-penelitian terdahulu yang memiliki kaitan dengan permasalahan hukum yang dianalisa oleh penulis, beberapa penelitian tersebut yaitu: pertama, "Ekuilibrium Pengaturan Perlindungan Data Pribadi Sebagai Jaminan Hak Konstitusional: Refleksi Implementasi di Masa Pandemi Covid-19".[11] Perbedaan dengan penelitian penulis yaitu pembahasan hanya menjabarkan secara umum pada hukum konstitusi secara umum, sedangkan penulis menjabarkan lebih spesifik pada beberapa undang-undang yang juga mempunyai pasal-pasal yang berkaitan dengan perlindungan data pribadi. Kedua, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber".[12] Perbedaan dengan pembahasan penulis yaitu terletak pada konsep perlindungan hukum yang diberikan. Konsep yang diberikan dalam penelitian tersebut yaitu terkait perlindungan hukum atas penyalahgunaan data pribadi serta peran penegak hukum dalam lingkup hukum pidana, sedangkan penulis lebih membahas terkait pengaturan-pengaturan hukum yang ada di Indonesia kemudian membandingkan dengan pengaturan hukum yang ada di Malaysia dan Singapura, sebagai gambaran terkait keamanan dan perlindungan hukum bagi konsumen *e-commerce*.

---

[9] Imantoko Kurniadi, *Op. Cit.*

[10] Yan Andriariza, et al, Strategi Implementasi Regulasi Perlindungan Data Pribadi di Indonesia, (Jakarta: Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika, 2019), hlm. 2

[11] Ahmad Habib Al Fikry, "Ekuilibrium Pengaturan Perlindungan Data Pribadi Sebagai Jaminan Hak Konstitusional: Refleksi Implementasi di Masa Pandemi Covid-19", *Seminar Nasional Hukum Universitas Negeri Semarang,* 7(1), hlm. 21-40.

[12] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber", *Jurnal Sasi,* Vol. 27 No. 1, hlm. 38-52

**Kosmik Hukum Vol.** 22 No. 1 (2022): 27-39
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v22i1.12154

## II. Rumusan Masalah

Berdasarkan isu hukum di atas, terdapat 2 (dua) rumusan masalah yang akan dibahas dalam penelitian ini, yaitu:

1. Apa bentuk perlindungan hukum data pribadi pengguna *e-commerce* di Indonesia?
2. Bagaimana perbedaan perlindungan data pribadi Indonesia dengan perlindungan data pribadi Malaysia dan Singapura ?

## III. Metode Penelitian

Jenis penelitian yang digunakan dalam meneliti isu hukum ini adalah penelitian hukum normatif. Pendekatan penelitian yang digunakan oleh penulis adalah pendekatan perundang-undangan (*statue approach*), pendekatan konseptual dan pendekatan perbandingan (*comparative approach*). Bahan hukum primer yang digunakan untuk menelaahh isu hukum ini yaitu Undang-Undang Dasar Tahun 1945, Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah menjadi Undang-Undang Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan, Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 28 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, *Personal Data Protection Act* 2010 Malaysia, dan *Personal Data Protection Act* 2012 sebagaimana telah diamandemen pada tahun 2020 Singapura. Bahan hukum sekunder yang digunakan yaitu berlandaskan teori-teori, konsep-konsep, literatur dan jurnal hukum yang mempunyai hubungan atau keterkaitan dengan permasalahan hukum yang dibahas dalam penelitian ini. Penulisan ini dibuat dengan membuat kerangka topik terlebih dahulu, kemudian mengumpulkan bahan-bahan hukum yang relevan. Bahan hukum tersebut selanjutnya dilakukan analisis dan dimasukkan ke dalam materi pembahasan.

## IV. Hasil dan Pembahasan

### 1. Bentuk Perlindungan Hukum Data Pribadi Pengguna e-Commerce di Indonesia

Berkaitan dengan teori perlindungan hukum, terdapat beberapa ahli yang menerangkan hal ini, diantaranya Fitzgerald, Satjipto Raharjo, Phillipus M Hanjon. Fitzgerald mengutip istilah teori perlindungan hukum dari Salmond bahwa:

> "Hukum bertujuan mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat karena dalam suatu lalulintas kepentingan, perlindungan terhadap kepentingan tertentu dapat dilakukan dengan cara membatasi berbagai kepentingan di lain pihak"

Kepentingan hukum yang dimaksud adalah mengurusi hak dan kepentingan manusia, sehingga hukum mempunyai otoritas tertinggi untuk menentukan kepentingan manusia yang perlu diatur dan dilindungi.[13] Menurut Satjipto Rahardjo, Perlindungan ihukum adalah imemberikan pengayoman terhadap hak asasi manusia (HAM) "yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh" hukum.[14] Selanjutnya menurut Phillipus M. Hadjon bahwa perlindungan hukum bagi rakyat sebagai tindakan pemerintah yang bersifat preventif dan resprensif. Perlindungan hukum yang preventif bertujuan untuk mencegah terjadinya sengketa, yang mengarahkan tindakan

[13] Satjipto Raharjo, *Ilmu Hukum*, (Bandung: PT. Citra Aditya Bakti, 2000), hlm. 53.
[14] *Ibid*, hlm. 69.

pemerintah bersikap hati-hati dalam pengambilan keputusan berdasarkan diskresi dan perlindungan yang resprensif bertujuan untuk mencegah terjadinya sengketa, termasuk penanganannya di lembaga peradilan.[15]

Berdasarkan penjelasan di atas memberikan pemahaman bahwa perlindungan hukum merupakan gambaran dari bekerjanya fungsi hukum untuk mewujudkan tujuan-tujuan hukum, yakni keadilan, kemanfaatan dan kepastian hukum. Perlindungan hukum adalah suatu perlindungan yang diberikan kepada subyek hukum sesuai dengan aturan hukum, baik itu yang bersifat preventif maupun dalam bentuk yang bersifat represif, baik yang secara tertulis maupun tidak tertulis dalam rangka menegakkan peraturan hukum. Bentuk perlindungan hukum di Indonesia tetap perlu dilakukan analisa untuk mengetahui sejauh mana hukum telah bekerja terutama mengenai perlindungan hak privasi yang juga mencakup didalamnya mengenai data pribadi. Sebelum membahas mengenai hak privasi di Indonesia, penting kiranya mengetahui sedikit sejarah perlindungan hak atas suatu privasi seseorang di Amerika dan Eropa yang juga mempunyai kaitan dengan perlindungan data privasi di Indonesia.

Perdebatan mengenai pentingnya perlindungan terhadap hak atas suatu privasi seseorang yang melekat pada diri pribadi muncul ke permukaan setelah adanya putusan-putusan pengadilan di Inggris dan Amerika Serikat, yang selanjutnya Samuel Warren dan Louis iBrandeis menuliskan sebuah konsepsi hukum tentang hak atas privasi dalam jurnal yang berjudul "*The Right to Privacy*" diterbitkan pada bulan Desember 1980[16]. Warrendan Brandeis memberikan definisi yang sederhana mengenai hak atas privasi yaitu "*the right to be let alone*" atau jika diterjemahkan dalam bahasa Indonesia berarti "hak untuk dibiarkan sendiri". Definisi tersebut berlandaskan pada 2 (dua) asas yaitu kerhormatan pribadi dan nilai-nilai seperti martabat individu, otonomi dan kemandirian pribadi[17]. Konsep di atas selanjutnya memperoleh justifikasi serta pengakuan semenjak adanya gugatan-gugatan hukum yang memberikan pembenaran mengenai pentingnya perlindungan hak atas privasi, terlebih berlandaskan pada aspek moralitas. Alan Westin juga mendefinisikan hak atas privasi sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri tentang kapan, bagaimana serta sampai sejauh mana informasi tentang mereka disebarkan kepada orang lain[18], sedangkan Solove menerangkan bahwa konteks privasi mencakup keluarga, tubuh, jenis kelamin, rumah serta komunikasi dan informasi pribadi seseorang[19]. Berdasarkan beberapa pendapat di atas tentang "privasi", dapat dikatakan bahwa privasi sebagai klaim, hak, atau hak individu untuk menentukan informasi apa saja tentang dirinya yang bisa dikomunikasikan kepada orang lain. Privasi juga telah diidentifikasi sebagai ukuran kontrol individu terhadap sejumlah elemen kehidupan pribadinya yang mencakup : informasi tentang diri peribadinya, kerahasiaan identitas pribadinya, serta pihak yang mempunyai akses terhadap pribadi tersebut[20].

Berbeda dengan Amerika Serikat, Pemerintah Eropa lebih memfokuskan pada aspek perlindungan data pribadi (sering disebut "data") sebagai bagian dari perlindungan kehidupan pribadi. Pengertian tersebut didasarkan pada Pasal 8 Konvensi Eropa yang telah menghasilkan beberapa penafsiran tentang cakupan dari kehidupan pribadi. Berdasarkan Pasal 8 Konvensi Eropa, yang termasuk ruang lingkup kehidupan pribadi mencakup : akses ke data pribadi, intersepsi komunikasi, pilihan atau perubahan nama, kehidupan seksual, profesi atau domisili, perlindungan terhadap gangguan lingkungan, serta hak untuk membangun dan mengembangkan hubungan dengan orang lain[21].

---

15 *Ibid*, hlm. 53.

16 Wahyudi Djafar, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaharuan", dari laman https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf, diakses tanggal 28 Oktober 2021

17 *Ibid*.

18 *Ibid*.

19 Daniel J. Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008),

20 Ferdinand Schoeman, "*Privacy: Philosophical Dimensions*", dalam Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984), hlm. 2.

21 Wahyudi Djafar, *Op. cit.,* hlm. 4

**Kosmik Hukum Vol.** 22 No. 1 (2022): 27-39
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v22i1.12154

Negara yang mengawali penerbitan mengenai aturan perlindungan data adalah Jerman pada Tahun 1970, yang selanjutnya disusul oleh Inggris, dan beberapa negara Eropa lainnya, seperti Swedia, Prancis, Swiss dan Austria. Amerika Serikat juga mulai menerbitkan beberapa pasal yang berisi perlindungan data di Undang-Undang Pelaporan Kredit yang adil di tahun yang sama. Hukum perlindungan data semakin berkembang pesat sejak Uni Eropa melakukan unifikasi hukum perlindungan data melalui peraturan perlindungan data umum Uni Eropa (EU GDPR-*General Data Protection Regulation)* di tahun 2016, dan selanjutnya diberlakukan pada tanggal 25 Mei 2018.[22] GDPR bersifat komprehensif, karena meliputi hampir seluruh pemrosesan data pribadi. Penerapannya pun tidak hanya akan berpengaruh pada pengendali serta prosesor data yang ada di Uni Eropa, melainkan dapat pula melakukan penawaran barang atau jasa dan/atau memantau perilaku individu warga negara Uni Eropa[23].

Sejak ditetapkannya sebagai hukum nasional hingga Januari 2018, kurang lebih 100 negara telah mengadopsi undang-undang perlindungan data, yang pada umumnya memuat tentang : ruang lingkup serta jangkauan dari perlindungan data, seperti pengendali dan prosesor data serta jangkauan teritorial/yuridiksi, pengertian serta jenis data pribadi, prinsip-prinsip perlindungan data, kewajiban pengendali dan prosesor data, hak-hak dari pemilik data, serta pengawasan dan penegakan undang-undang yang pada umumnya dilengkapi dengan *independent supervisory authority (data protection authority).*[24]

Regulasi khusus mengenai perlindungan data pribadi di Indonesia belum diatur secara komprehensif seperti di Eropa maupun Amerika, akan tetapi ketentuan mengenai jaminan terhadap perlindungan hak privasi yang juga menyangkut data pribadi bisa dilihat di dalam substansi Pasal 28G ayat (1) UUD 1945 yang berbunyi : "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi", selain ketentuan tersebut, turut sertanya Indonesia sebagai pihak dari *International Covenant on Civil and Political Rights* (ICCPR), yang selanjutnya disahkan melalui Undang-Undang Nomor 12 Tahun 2005 Tentang Pengesahan *International Covenant on Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik) merupakan bentuk pemerintah Indonesia berusaha menjaga dan menjamin perlindungan data pribadi warga negaranya.

Perlindungan data pribadi di Indonesia sejatinya ada, akan tetapi tidak memberikan kepastian yang begitu jelas dalam memberikan perlindungan kepada masyarakat. Regulasi mengenai data pribadi ini belum diatur secara spesifik dalam satu undang-undang namun terdapat beberapa pasal yang tersebar dalam beberapa undang-undang. Perlindungan hak privasi yang mencakup data pribadi di Indonesia dapat ditemui dalam Pasal 14 ayat (2), Pasal 29 ayat (1) dan Pasal 31 Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia (UU HAM). Ketiga pasal tersebut pada intinya menerangkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya. Perlindungan yang dimaksud bukan sekedar dalam arti hubungan langsung, namun atas informasi atau data pribadi juga. Pasal 31 UU HAM juga mengatur mengenai jaminan kemerdekaan rahasia dalam hubungan komunikasi melalui sarana elektronik, kecuali atas perintah hakim atau kekuasaan lain yang sah menurut ketentuan perundang-undangan[25]. Regulasi mengenai perlindungan data pribadi juga dapat ditemukan dalam ketentuan Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah menjadi Undang-Undang Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan (UU Administrasi Kependudukan). Hal tersebut dapat dilihat dari definisi data pribadi yang dijelaskan dalam Pasal 1 ayat (22) yang berbunyi : "data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya." Pasal 2 huruf (c) menegaskan mengenai salah satu hak penduduk yaitu mendapatkan

[22] *Ibid*.
[23] *Ibid*.
[24] *Ibid*.
[25] *Ibid*.

perlindungan atas data pribadi dan ditegaskan pula pada Pasal 2 huruf (f) bahwa apabila terjadi kesalahan atau penyalahgunaan data pribadi oleh instasni pelaksana maka penduduk dapat mengajukan ganti rugi dan pemulihan balik nama ke oknum instansi pelaksana yang bersangkutan. Adapun data pribadi penduduk yang harus dilindungi menurut ketentuan Pasal 84 ayat (1), yaitu : "a. nomor Kartu Keluarga (KK); b. Nomor Induk Kependudukan (NIK); c. tanggal, bulan, tahun lahir; d. keterangan tentang kecacatan fisik dan/atau mental; e. NIK ibu kandung dan ayah; f. beberapa isi catatan peristiwa penting, selain itu terdapat pula sidik jari, iris mata, tanda tangan dan elemen data lainnya yang merupakan aib seseorang."

Perlindungan data pribadi dapat pula ditemui dalam sektor keuangan sejak diterbitkannya Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan. Sejak adanya regulasi tersebut Otoritas Jasa Keuangan (OJK) mempunyai wewenang dalam mengawasi segala bentuk kegiatan penyelenggaraan jasa keuangan. Pengawasan tersebut meliputi kerahasiaan data pribadi nasabah yang ditekankan lagi dalam Peraturan OJK Nomor 1/POJK.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan, selanjutnya OJK mengatur mengenai perlindungan data pribadi lebih rinci lagi melalui Surat Edaran OJK Nomor 14/SEOJK.07/2014 Tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen, meliputi nama, alamat, nomor telepon, tanggal lahir dan/atau umur, dan/atau nama ibu kandung (khusus nasabah perorangan), serta susunan direksi dan komisaris termasuk dokumen identitas berupa KTP/paspor/izin tinggal dan/atau susunan pemegang saham (khusus untuk nasabah korporasi)[26]. Apabila mencermati beberapa peraturan perundang-undangan yang lain, ditemukan beberapa pasal yang menyinggung mengenai pengaturan data pribadi di Indonesia, akan tetapi pengaturan data pribadi yang ditemukan dibeberapa regulasi hukum tersebut masih bersifat universal (umum) dan fokus pada sektor masing-masing, sehingga tidak memberikan jaminan perlindungan secara terpenuh dan menyeluruh kepada mereka yang data pribadinya dilanggar oleh oknum yang tidak bertanggung jawab terutama perlindungan data pribadi di era teknologi informasi yang kian hari terus berkembang.

Mengingat dunia sekarang semakin maju dengan perkembangan teknologi informasi, menambah was-was akan kebocoran-kebocoran data pribadi yang semakin mudah diperoleh oleh pelaku-pelaku kejahatan siber, salah satunya pencurian data dari platform *e-commerce.* Hal tersebut dikarenakan syarat umum untuk memakai platform *e-commerce* harus melakukan pendaftaran dengan menggunakan identitas KTP, Nomor telepon, dan *e-mail. E-commerce* merupakan aktivitas bisnis yang berhubungan dengan konsumen (*consumers),* manufaktur (*manufacturs*), *service providers,* dan pedagang perantara (*intermediateries)* dengan menggunakan jaringan-jaringan komputer (*computer networks),* yaitu *e-commerce* telah mencakup semua *spectrum* aktivitas komersial[27]. Transaksi *e-commerce* melibatkan para pihak yaitu penjual (*merchant)*, pembeli (*card holder*), perantara penagihan (*acquirer*), penerbit kartu kredit (*issuer)*, *certification authorities,* dan jasa pengiriman atau ekspedisi, selanjutnya keseluruhan pihak tersebut dalam disebut juga pengguna *e-commerce*[28]. Rentannya tindak kejahatan siber dalam dunia teknologi informasi mengharuskan adanya perlindungan hukum hak suatu privasi seseorang yaitu berupa data pribadi, apabila di kemudian hari terdapat potensi kebocoran data pribadi.

Perlindungan data pribadi di Indonesia dalam konteks teknologi informasi dapat ditemui idalam Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 28 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Sektor Pemerintah Indonesia yang terfokus dalam penanganan *e-commerce* adalah Kementrian Komunikasi dan Informasi (Kominfo)[29]. Berdasarkan kedua aturan di atas, Kominfo mempunyai program pendaftaran dan pendataan untuk pelaku usaha *e-*

---

[26] *Ibid*.

[27] Niniek Suparni, *Cyberspace Problematika & Antisipasi Pengaturannya*, (Sinar Garfika, Jakarta, 2009), hlm. 3.

[28] Dianne Eka Rusmawati, "Perlindungan Hukum Bagi Konsumen dalam Transaksi *e-Commerce*", *Fiat Justisia Jurnal Ilmu Hukum,* Vol. 7 No. 2, (2013): hlm. 195-197

[29] I Putu Bayu Mahendra dan I Dewa Gede Dana Sugama, "Perlindungan Data Pribadi Konsumen Daring Pada Saat Bertransaksi *E-Commerce* di Indonesia", *Jurnal Kertha Desa,* Vol. 8 No. 12, 2020, 42

**Kosmik Hukum Vol.** 22 No. 1 (2022): 27-39
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v22i1.12154

*commerce* melalui serangkaian proses *profiling* dan *report database*.[30] Hal tersebut berguna untuk menghindarkan para konsumen dari kejahatan penipuan.

Bentuk perlindungan data pribadi melalui UU ITE terdapat dalam ketentuan Pasal 26 ayat (1) dan ayat (2) yang memuat tentang persetujuan dari subjek data sebelum data pribadinya dilakukan pengolahan, serta memberikan hak kepada subjek untuk mengakses dan mengontrol pengolahan data pribadi mereka. Secara detail bunyi pasal di atas yaitu :

"Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."

"Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Apabila ditinjau berdasarkan teori perlindungan hukum, perlindungan data pribadi yang diatur dalam beberapa regulasi diatas belum memberikan perlindungan hukum yang paripurna, karena hukum yang mengatur perlindungan data pribadi masih belum komprehensif dan tersebar di beberapa regulasi, selain itu pengaturan mengenai perlindungan data pribadi hanya diatur pada peraturan pelaksana tanpa sanksi yang tegas. Mengingat problematika kebocoran data yang ada di *e-commerce* selalu terjadi secara masif, membuktikan bahwa regulasi di atas kurang dalam memberikan perlindungan hukum, sedangkan UU ITE hanya mencakup perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interfensi ilegal[31]. Konsep perlindungan hukum di Indonesia masih tidak cukup dalam melindungi data pribadi dalam sistem elektronik, karena aturan tersebut tidak mengatur serta mencakup mengenai aktivitas pertukaran data yang legal[32].

Berdasarkan penjelasan di atas, maka urgensi dari perlindungan data pribadi kian hari kian dibutuhkan khususnya untuk memberikan perlindungan data pribadi untuk pengguna *e-commerce* di Indonesia. Pemerintah Indonesia hingga saat ini belum mempunyai regulasi yang komprehensif (dalam satu undang-undang) mengenai perlindungan data pribadi, walaupun dalam prolegnas Dewan Perwakilan Rakyat (DPR) telah mencanangkan dana pemerintah guna pengusulan draft awal tentang Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)[33]. Keikutsertaan Indonesia dalam beberapa perjanjian dagang, yang juga membicarakan masalah *e-commerce* dengan isu *cross border data flows* menambah keharusan Indonesia untuk segera melakukan pembaharuan hukum dengan mengesahkan RUU PDP guna memberikan keamanan data dalam negeri. Terlebih lagi, setelah berlakunya EU GDPR pada tahun 2018 yang juga memiliki pengaruh yang signifikan bagi perusahaan yang berkecimpung di berbagai sektor, salah satunya adalah *e-commerce.* Urgensi mengenai penerbitan RUU PDP juga mengingat gerakan 1000 *start up* yang dicanangkan oleh Presiden Joko Widodo sebagai salah satu dasar untuk mengembangkan ekonomi digital, yang sukses menumbuhkan 4 (empat) *start up* unicorn yaitu Tokopedia, Bukalapak, Traveloka dan Go-Jek. Program tersebut secara langsung menimbulkan pengumpulan data pribadi konsumen secara besar-besaran dan berpotensi adanya ancaman kebocoran data, bahkan di tahun 2020 telah banyak data-data dari perusahaan *e-commerce* telah dicuri dan dijual secara ilegal.

## 2. Perbedaan Perlindungan Data Pribadi Indonesia dengan Perlindungan Data Pribadi Malaysia dan Singapura

Merespon perkembangan ekonomi digital salah satunya di bidang *e-commerce*, beberapa negara ASEAN lebih awal telah menerbitkan aturan khusus mengenai perlindungan data seperti Malaysia pada tahun 2010, Singapura dan Filipina pada tahun 2012, Laos tahun 2017 dan

---

30 *Ibid*.

31 Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum,* Vol. 10 No. 2, (2019): hlm. 222.

32 *Ibid*, hlm. 221-222

33 *Ibid*

Thailand pada tahun 2019[34]. Malaysia merupakan negara anggota ASEAN yang pertama kali menerbitkan UU PDP dengan berprinsip pada perlindungan data pribadi *The Organization for Economic and Cooperation Development* (OECD) yang merupakan organisasi internasional yang bergerak dibidang kerjasama ekonomi dan pembangunan.

Prinsip-prinsip tersebut adalah : "(i) Prinsip Pengumpulan Batasan *(Collerction Limitation Prinsiple)*, yaitu adanya batasan dalam melakukan pengumpulan data pribadi secara sah dan adil, serta diikuti persetujuan dari subyek data dan dengan sepengetahuannya; (ii) Prinsip Kualitas *(Data Quality Principle)*, yaitu data pribadi yang diambil harus lengkap, akurat dan sesuai dengan maksud pemakaian serta jika data pribadi tersebut mengalami perubahan, maka harus dilakukan pembaharuan dengan cepat; (iii) Prinsip Tujuan Khusus *(Purpose Specification Principle)*, yaitu tujuan pengumpulan data pribadi harus ditentukan paling lambat pada saat data pribadi dikumpulkan, selanjutnya terbatas pada tujuan; (iv) Prinsip Batasan Penggunaan *(Use Limitation Principle)*, maksudnya pemilik data harus memberikan persetujuan pemilik data pribadi mengenai pengungkapan, atau penggunaan data untuk maksud selain tujuan awal data tersebut dikumpulkan; (v) Prinsip Perlindungan Keamanan (*Security Safeguard Principle*), data pribadi harus mendapatkan perlindungan dari resiko kehilangan dan perusakan data, penggunaan tanpa ijin, pengungkapan data maupun akses yang tidak sah; (vi) Prinsip Keterbukaan *(Openness Principle*), yaitu Tujuan utama penggunaan data, identitas serta pengontrol data harus dibangun, sebelumnya harus dibentuk kebijakan tentang keterbukaan terkait pengembangan atau pengelolaan yang berkaitan dengan data pribadi; (vii) Prinsip Partisipasi Individu (*Individual Participation Principle)*, Tujuan dari prinsip ini adalah untuk mengontrol data atau mengkonfirmasi data yang terkait dengannya dengan memberikan akses untuk dapat dihapus, diubah maupun diperbaiki; dan (viii) Prinsip Akuntabilitas *(Accountability Principle),* Pengontrol data harus bertanggung jawab untuk mematuhi langkah-langkah yang berdampak pada prinsip-prinsip yang disebutkan di atas."[35]

Prinsip-Prinsip di atas selanjutnya dicantumkan dalam substansi UU PDP Malaysia yang selanjutnya dikenal dengan *Personal Data Protection Act* 2010. UU tersebut berlaku sejak tahun 2013, yang substansinya memberikan pengaturan secara rinci dan tegas mengenai prinsip-prinsip perlindungan data pribadi, hak-hak pemilik data, tata cara pemindah tanganan data, serta kewajiban bagi pihak yang melakukan penyimpanan data, serta mengatur mekanisme komplain bagi seseorang yang data pribadinya dipindah tangankan secara tidak sah.[36] Prinsip perlindungan data pribadi yang di atur di dalam *Personal Data Protection Act 2010* tercermin dengan dibentuknya Komita Penasihat Perlindungan Data Pribadi yang mempunyai tugas untuk menerima dan menampung laporan atau aduan apabila terdapat oknum yang menyalahgunakan dan memindahtangankan data pribadi secara melawan hukum, selain itu terdapat pula pengadilan banding guna menyelesaikan permasalahan yang berkaitan dengan data pribadi secara yudisial. UU PDP Malaysia juga sangat tegas dalam menindak pelaku dengan ancaman pidana bagi siapa saja yang melanggar peraturan tersebut, seperti sanksi yang dijatuhkan kepada oknum atau siapa saja yang tanpa izin melakukan pengaksesan atau pengumpulan data pribadi secara melawan hukum, maka pelaku dapat dipidana denda maksimal lima ratus ribu ringgit Malaysia dan/atau penjara maksimal tiga tahun.

UU PDP Malaysia juga mempunyai 7 (tujuh) prinsip perlindungan data pribadi yang tertuang dalam *section* I5 (1), yaitu "prinsip umum (*the general principle),* prinsip pemberitahuan dan pilihan (*the notice and choice principle),* prinsip pengungkapan (*the disclosure prinsiple)*, prinsip keamanan (*the security principle),* prinsip retensi (*the retention prinsiple),* prinsip integritas data (*the data integrity principle)*, dan prinsip akses (*the access principle)".* Prinsip di atas bersifat kumulatif, artinya semua prinsip di atas harus terpenuhi supaya dapat memberikan perlindungan atas data pribadinya dan bagi siapa saja yang melanggar prinsip tersebut, maka akan dikenakan denda tiga ratus ribu ringgit atau dipenjara selama dua tahun.

---

[34] Wahyudi Djafar, *Op. Cit*, hlm. 13
[35] Muhammad Saiful Rizal, *Op.Cit*., hlm. 222-223.
[36] *Ibid*.

**Kosmik Hukum Vol.** 22 No. 1 (2022): 27-39
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v22i1.12154

Guna memberikan perlindungan data secara maksimal, UU PDP Malaysia mempunyai aturan terkait aplikasi pendaftaran yang diatur di dalam *section* 16 (1) yaitu : "Seseorang yang termasuk dalam kelas pengguna data sebagaimana ditentukan dalam urutan yang dibuat berdasarkan ayat 14 (1) harus mengajukan permohonan pendaftaran kepada komisaris dengan cara dan formulir sebagaimana ditentukan oleh komisaris." Berdasarkan aturan tersebut maka setiap pelaku usaha maupun pengguna data wajib melakukan pendaftaran aplikasinya kepada komisaris yang selanjutnya komisaris menerbitkan sertifikat pengolahan data. Pelaku usaha atau pengguna data yang melakukan pemrosesan data pribadi tanpa mengantongi sertifikat dapat dikenai denda lima ratus ribu ringgit atau dipenjara selama tiga tahun.[37]

Keunggulan lain dari UU PDP Malaysia ini juga mengatur terkait transfer data lintas batas (*cross-border transfer)*, namun transfer data tersebut terbatas pada negara yang mempunyai tingkat perlindungan data pribadi yang sama atau setara dengan Malaysia, baik dari segi aturan dan juga sarana dan prasarananya[38]. Hal tersebut bertujuan untuk melindungi data pribadi warganya agar tidak mengalami kebocoran dan penyalahgunaan data oleh pihak lain. Aturan mengenai transfer data diatur di dalam *section* 129 ayat (1) yang menerangkan bahwa : "Pengguna data tidak boleh mentransfer data pribadi apa pun dari suatu subjek data ke suatu tempat di luar Malaysia kecuali ke tempat seperti yang ditentukan oleh Menteri, atas rekomendasi Komisaris, dengan pemberitahuan yang diterbitkan dalam Lembaran Berita."

Selain Malaysia, Singapura juga mempunyai aturan berupa *Personal Data Protection Act* 2012 yang juga baru saja di amandemen pada tahun 2020 (UU PDP Singapura) . Regulasi tersebut berlaku sejak awal tahun 2014. Ketentuan yang diatur di dalam UU PDP Singapura mempunyai banyak kesamaan, sebab kedua aturan tersebut telah mengadopsi aturan yang ada di dalam *European Data Protective Directive* (EUDP). UU PDP Singapura mempunyai sedikit perbedaan dengan UU PDP Malaysia. UU PDP Singapura mempunyai aturan khusus untuk membentuk sebuah badan khusus pendaftaran nomor telepon bernama *Do Not Call (DNC) Registry*, sehingga masyarakat memiliki hak untuk menerima maupun menolak pesan singkat (SMS atau MMS) dari pihak ataupun organisasi *marketing* yang tidak diinginkan, sedangkan di Malaysia tidak ada mengenai aturan demikian[39].

Singapura mempunyaii aturan yang ketat dan tegas mengenai perlindungan data pribadi di negaranya baik di lingkup pemerintahan maupun dilingkup pihak swasta. Pada lingkup organisasi atau pihak swasta di Singapura, diwajibkan untuk memberikan jaminan keamanan data yang tersimpan di bawah kontrolnya maupun pada aplikasi *SafeEntry.* Hal tersebut diatur di dalam *section 24 Personal Data Protection Act* yang pada pokoknya mewajibkan organisasi atau pihak swasta untuk melindungi data pribadi dengan aman dan melakukan pencegahan terhadap akses, pengumpulan, penggunaan, pengungkapan yang tidak sah, dan hilangnya media atau perangkat penyimpanan data pribadi[40]. Apabila terjadi kebocoran data *(disclosure of data)* secara tidak sah di naungan organisasi atau pihak swasta, maka *section 48* mengatur sanksi yang dapat menjerat organisasi tersebut akibat kelalaian atau kesengajaan yang dilakukan. Manakala terjadi *unauthorized disclosure of data*, individu di bawah organisasi tersebut dapat dikenakan pidana penjara sampai dengan 2 tahun dan/atau dikenakan denda sebesar $5,000 dollar Singapura.

Sama halnya dengan Malaysia, guna memberikan perlindungan data pribadi secara efektif dan maksimal, Singapura membentuk sebuah komisi yang dapat disebut sebagai *Personal Data Protection Commission* (PDPC).[41] Komisi tersebut mempunyai kewenangan dalam mengawasi kepatuhan dalam implementasi aturan ini, selain itu juga memiliki wewenang menerima laporan atau aduan masyarakat umum, serta sebagai fasilitator dalam penyelesaian sengketa alternatif.

---

37 *Ibid*, hlm. 224.

38 Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia". *Kanun: Jurnal Ilmu Hukum*, Vol. 20, hlm. 379.

39 Nadia Tsamara, "Perbandingan Aturan Perlindungan Privasi atas Data Pribadi antara Indonesia dengan Beberapa Negara", *Jurnal Suara Hukum,* Vol, 3 No. 1, (2021): hlm. 73.

40 Tiara Almira R., Sinta D. R., Rika R. P., "Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan Covid-19 Serta Tanggung Jawabnya", *Jurnal Kepastian Hukum dan Keadilan,* Vol. 2 No. 1, (2020): hlm. 12-13.

41 *Ibid*, hlm. 14.

Bagi siapa saja yang mengalami kerugian karena penyalahgunaan data privasinya oleh organisasi atau pihak swasta dapat melakukan aduan ke PDPC, selanjutnya PDPC melakukan penyidikan dan apabila terdapat cukup bukti, maka berdasarkan *section* 56 UU PDP Singapura dapat dijatuhi sanksi berupa denda mencapai satu juta dollar Singapura dan/atau penjara maksimal tiga tahun penjara.

Berbeda dengan Malaysia dan Singapura, aturan di Indonesia mengenai perlindungan data privasi dibidang elektronik, seperti yang telah dijelaskan pada sub-bab sebelumnya diatur secara universal di UU ITE yang selanjutnya terdapat aturan pelaksananya berupa PP PTSE. Pasal 15 PP PTSE mewajibkan semua penyelenggara sistem elektronik untuk menjaga data pribadi yang di bawah pengelolaannya. Pasal 15 ayat (3) PP PSTE, selanjutnya mendelegasikan kepada Menteri Komunikasi dan Informatika untuk mengeluarkan peraturan berupa Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (selanjutnya disebut Permenkominfo 20/2016). Peraturan ini lebih komprehensif mengatur perlindungan data pribadi, seperti dalam hal persetujuan pemilik data (terdapat pada Pasal 9), tujuan pengumpulan data (terdapat pada Pasal 7), pembatasan (terdapat pada Pasal 7 Jo. Pasal 12), pencegahan (terdapat pada Pasal 5), pilihan (terdapat pada Pasal 8), penyimpanan data (terdapat pada Pasal 15), pengungkapan data (terdapat pada Pasal 21 Jo. Pasal 23), transfer data (terdapat pada Pasal 22), serta pemberitahuan (terdapat pada Pasal 28). Sayangnya, aturan yang ada dalam Permenkominfo tidak dibarengi dengan adanya sanksi pidana. Penegakan hukumnya hanya berupa sanksi administratif, meskipun sanksi pidana adalah *ultimum remedium*, akan tetapi sanksi tersebut dianggap cukup efektif dalam memberikan efek jera terhadap pelaku penyalahgunaan data pribadi.[42] Dapat dikatakan bahwa pengaturan khusus mengenai perlindungan data pribadi yang hanya pada sebatas Peraturan Menteri kurang dapat mengakomodir permasalahan menyangkut data pribadi yang demikian kompleks khususnya dalam bidang *e-commerce*, hal tersebut terbukti dengan adanya banyak kasus kebocoran data yang terjadi di beberapa perusahaan *e-commerce* raksasa di Indonesia.

Berdasarkan penjelasan di atas, maka kelebihan-kelebihan UU PDP yang telah diimplementasikan di Malaysia dan Singapura, dapat di adopsi oleh Indonesia dalam RUU PDP. Hal tersebut dilakukan guna bisa memberikan gambaran mengenai regulasi dan implementasi perlindungan data pribadi yang efektif dan menimbulkan efek jera, sehingga pelaku tidak meremehkan atau menyepelekan lagi mengenai data pribadi warga negara Indonesia.

## V. Penutup

Perlindungan data pribadi di Indonesia terutama di era digital saat ini adalah suatu kebutuhan yang sangat urgen, mengingat banyaknya kebocoran data di beberapa perusahaan *e-commerce* Indonesia. Regulasi mengenai perlindungan data di Indonesia masih tersebar di beberapa peraturan perundangan-undangan dan tidak bersifat komprehensif, salah satunya yaitu di atur di dalam UU ITE. UU ITE mempunyai regulasi turunan hingga munculnya peraturan menteri yang mengatur tentang perlindungan data secara elektronik, akan tetapi aturan tersebut tidak memberikan perlindungan data secara tegas.

Pelindungan data pribadi di Indonesia jauh tertinggal dengan aturan-aturan di beberapa negara ASEAN seperti Malaysia dan Singapura. Malaysia dan Singapura mempunyai regulasi khusus dan komprehensif dalam mengatur perlindungan data pribadi warganya yaitu berupa UU PDP Malaysia dan Singapura yang juga menyesuaikan dengan aturan EU GDPR guna memperketat keamanan data yang dikelola oleh pihak swasta dan memberi sanksi tegas bagi siapa saja yang mengakses, mengumpulkan, dan menstransfer data dengan cara tidak sah atau melawan hukum. Indonesia perlu segera melakukan pembaharuan hukum mengenai perlindungan data dengan membentuk atau menerbitkan regulasi setingkat Undang-Undang yang mengatur secara komprehensif tentang perlindungan data pribadi seperti Malaysia atau Singapura. Hal tersebut sangat membantu perekonomian Indonesia khususnya dibidang *e-*

[42] *Ibid*, hlm. 12.

*commerce* mengingat transaksi perdagangan saat ini menggunakan data pribadi untuk dapat mengakses dan melakukan transaksi didalamnya. Adanya regulasi tersebut maka kekhawatiran mengenai pengelolaan data atau transfer data baik secara lokal bahkan lintas negara mempunyai keamanan yang ketat dan sanksi yang tegas, sehingga meminimalisir terjadinya pelanggaran ataupun penyalahgunaan dari oknum atau pihak yang tidak bertanggung jawab.

**Daftar Pustaka**

Akbar, Mohammad Aldrin dan Alam, Sitti Nur. *E-Commerce Dasar Teori dalam Bisnis Digital*. Medan: Yayasan Kita Menulis, 2020.

Al Fikry, Ahmad Habib. "Ekuilibrium Pengaturan Perlindungan Data Pribadi Sebagai Jaminan Hak Konstitusional: Refleksi Implementasi di Masa Pandemi Covid-19", *Seminar Nasional Hukum Universitas Negeri Semarang,* 7(1), 21-40.

Almira R., Tiara, Sinta D. R., Rika R. P.. "Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan Covid-19 Serta Tanggung Jawabnya", *Jurnal Kepastian Hukum dan Keadilan,* Vol. 2 No. 1, (2020), 1-16

Andriariza, Y. *et.al*., "Strategi Implementasi Regulasi Perlindungan Data Pribadi di Indonesia".Jakarta: Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika, 2019.

Djafar, Wahyudi. "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaharuan", dari laman https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf.

Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen", *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era,* (2020), 43-60

Hendra Wicaksana, Ratnadi. "Studi Kebijakan Perlindungan Data Pribadi dengan *Narrative Policy Framework*: Kasus Serangan Siber Selama Pandemi Covid-19", *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, Vol. 22 No. 2 (2020), 142–158.

Kominfo. Kemkominfo: Pertumbuhan *e-Commerce* Indonesia Capai 78 Persen, dari laman https://kominfo.go.id/content/detail/16770/kemkominfo-pertumbuhan-e-commerce-indonesiacapai-78-persen/0/sorotan_media; diakses pada 24 Oktober 2021

Kurniadi, Imantoko. Lazada Singapura Akui Kebobolan 1,1 Juta Data Pribadi Penggunanya, laman dari https://selular.id/2020/11/lazada-singapura-akui-kebobolan-11-juta-data-pribadi-penggunanya/; diakses tanggal 24 Oktober 2021

Mahendra, I Putu Bayu dan Sugama, I Dewa Gede Dana. "Perlindungan Data Pribadi Konsumen Daring Pada Saat Bertransaksi E-Commerce di Indonesia", *Jurnal Kertha Desa,* Vol. 8 No. 12, 2020, 39-46

Raharjo, Satjipto. *Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti, 2000.

Rizal, Muhammad Saiful. "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", *Jurnal Cakrawala Hukum,* Vol. 10 No. 2, (2019), 218-227.

Rongiyati, Sulasi. "Urgensi Sinergitas Pengaturan Pelindungan Data Pribadi dan Keamanan Siber Nasional", *Jurnal Info Singkat Bidang Hukum Pusat Penelitian Badan Keahlian DPR RI,* Vol. XIII No. 11/I/Puslit/Juni/2021, 1-6

Rusmawati, Dianne Eka. "Perlindungan Hukum Bagi Konsumen dalam Transaksi *e-Commerce*", *Fiat Justisia Jurnal Ilmu Hukum,* Vol. 7 No. 2 (2013), 193-201

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia". *Kanun: Jurnal Ilmu Hukum*, Vol. 20, 369-384

Schoeman, Ferdinand. "*Privacy: Philosophical Dimensions*", dalam Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, (Cambridge: Cambridge University Press, 1984)

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber", *Jurnal Sasi,* Vol. 27 No. 1, 38-52Solove, Daniel J. *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008)

Suparni, Niniek. *Cyberspace Problematika& Antisipasi Pengaturannya*. (Sinar Garfika, Jakarta, 2009)

Tsamara, Nadia. "Perbandingan Aturan Perlindungan Privasi atas Data Pribadi antara Indonesia dengan Beberapa Negara", *Jurnal Suara Hukum,* Vol, 3 No. 1, 2021, 53-85