PERLINDUNGAN HUKUM DATA PRIBADI PEMBELI DI PERDAGANGAN SECARA ELEKTRONIK (*E-COMMERCE*) DI INDONESIA

Etania Fajarani Halim
Fakultas Hukum, Universitas Pelita Harapan
etaniafhalim@gmail.com

Abstract
The development of technology, especially on information and telecommunication has encouraged the development of online businesses such as e-commerce. Due to the COVID-19 pandemic, people's lifestyles are switching and relying on shopping on e-commerce. The world economy is enormous by changes due to the development of financial, investment, production and trade. With the invention of e-commerce, buying and selling transactions can be carried out anytime and anywhere. However, this can also be used as a double-edged sword, because there are many possible crimes that occur in e-commerce transactions, such as data leakage. The last few years there have been several cases of data leakage. Nevertheless, there has been no resolution because there is no specific law for the protection of personal data. It is advisable to set up specific law for this protection of personal data for buyers who use e-commerce.

Keywords: *Personal Data Protection; Buyers; Electronic Commerce*

Abstrak
Perkembangan teknologi, khususnya teknologi informasi telah mendorong perkembangan bisnis daring seperti *e-commerce*. Adanya Pandemi COVID-19 juga telah mengubah gaya hidup masyarakat menjadi banyak melakukan belanja di *e-commerce*. Seiring dengan itu, perekonomian dunia mengalami perubahan yang sangat signifikan, baik di bidang finansial, investasi, maupun produksi dan perdagangan. Dengan adanya invensi *e-commerce*, transaksi jual beli dapat dilakukan kapan dan di mana saja. Namun hal ini juga menjadi pedang bermata dua, karena banyaknya kemungkinan kejahatan dalam transaksi *e-commerce,* termasuk kebocoran data. Penelitian ini menghasilkan temuan bahwa dalam beberapa tahun terakhir telah terjadi beberapa kasus kebocoran data. Namun tidak ada penyelesaian memadai karena belum ada aturan perlindungan data pribadi. Oleh karena itu, perlindungan hukum atas data pribadi bagi pembeli yang menggunakan *e-commerce* perlu segera diatur secara memadai.

Kata Kunci: Perlindungan Data Pribadi; Pembeli; Perdagangan Secara Elektronik

A. Pendahuluan

Indonesia adalah salah satu negara di Asia Tenggara yang memiliki perkembangan ekonomi tercepat di dunia, namun karena adanya pandemi Covid-19, Badan Pusat Statistik (BPS) mencatat adanya pertumbuhan ekonomi minus pada tahun 2020 yang terkontraksi selama 2,07%.[1] Kegiatan finansial, investasi, produksi dan perdagangan berdampak positif pada perkembangan perekonomian dunia dan menimbulkan persaingan yang ketat dan

[1] "Pertumbuhan Ekonomi Indonesia Triwulan IV 2020," *Bank Indonesia,* 5 February 2021, https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_233321.aspx.

globalisasi. Globalisasi telah menggabungkan ekonomi dunia sehingga praktik bisnis dan batas antar negara seakan-akan dianggap tidak ada.[2] Menurut Sander, globalisasi adalah proses di mana negara-negara mulai menghapuskan batasan sehingga tercipta dunia yang lebih terbuka dan tanpa batas.[3]

Karena adanya Pandemi Covid-19, masyarakat dihimbau untuk mengurangi bepergian dan di rumah saja maka dari itu memberikan dampak negatif pada daya beli di pasar yang mengakibatkan penurunan pendapatan usaha, volume transaksi dan kelancaran pendistribusian barang selama tahun 2020.[4] Dikarenakan hal ini, masyarakat mulai beralih dan mengandalkan pembelian secara daring melalui *e-commerce* untuk dapat memenuhi kebutuhan pokok mereka, pertumbuhan ini diakibatkan oleh adanya perkembangan infrastruktur dan penetrasi digital di Indonesia.[5]

Pada era ini, dunia sedang ada dalam abad di mana informasi mempunyai peran yang sangat penting dalam kehidupan manusia, seperti berdasarkan kemajuan informasi, komunikasi dan teknologi atau yang lebih dikenal dengan *Information Communication Technology* (ICT), merupakan salah satu faktor yang mendorong perkembangan ekonomi dunia. Karena perkembangan ICT, pada awal tahun 1990 diciptakannya perdagangan secara elektronik atau yang lebih dikenal sebagai *Electronic Commerce* atau *E-Commerce.*[6] *Electronic Commerce* adalah aktivitas jual beli yang dilakukan melalui elektronik dan internet. Menurut Wearesocial dan Hootsuite, sekitar 90% pengguna internet di Indonesia pernah melakukan transaksi daring dan hal ini mendukung Indonesia untuk menjadi pasar *e-commerce* terbesar di Asia Tenggara. Pada tahun 2019, nilai kapitalisasi pasar *e-commerce* di Indonesia mencapai USD 21 miliar dan menurut laporan McKinsey, pada tahun 2022 dapat mencapai USD 40 miliar.[7]

Karena adanya invensi *e-commerce* maka dapat meningkatkan efisiensi, mempermudah dan mengefektifkan waktu dan tempat sehingga transaksi jual beli dapat dilakukan dari mana saja dan kapan saja, dan melalui salah satu jenis *e-commerce* yaitu *marketplace*, di mana penjual memasang foto dan deskripsi dari produk yang dijual dan apabila pembeli setuju untuk membeli maka akan mentransfer dana ke *marketplace* tersebut dan penjual akan mengirimkan produknya. Apabila pembeli telah menerima produk dan sesuai dengan pesanan mereka,

[2] Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional* (Bandung: Widya Padjajaran, 2009), 1.
[3] *Ibid.*
[4] Bank Indonesia, *Loc. Cit.*
[5] Shinta Dewi, *Op. Cit.*, 2.
[6] *Ibid.*
[7] "Menilik Tren Perkembangan E-Commerce Indonesia di 2020," Sirclo, 19 August 2020, https://www.sirclo.com/blog/menilik-tren-perkembangan-e-commerce-indonesia-di-2020/.

pembeli akan mengkonfirmasi penerimaan produk dan dana penjual akan cair. Tetapi jika pembeli merasa kurang puas, atau ada produk yang tidak lengkap maka pembeli berhak untuk mengajukan komplain dan menunda pencairan uang ke penjual sampai masalah tersebut dapat terselesaikan oleh kedua belah pihak. Transaksi dapat dilakukan melalui internet dan media seperti *smartphone* atau laptop ini membuat pembeli dan penjual dapat melakukan transaksi tanpa tatap muka sehingga kontrak jual beli yang terjadi di antara kedua pihak dilakukan secara elektronik, dan ditandatangani secara *e-sign.*

Kontrak jual beli secara elektronik pada umumnya menggunakan sistem hukum yang fokus pada norma atau kaidah yang berlaku di negara tersebut. Tetapi berdasarkan beberapa ketentuan jual beli yang bersifat wajib dalam proses jual dan beli seperti hak dan kewajiban para pelaku transaksi ditegaskan dalam kesepakatan jual beli sebagai pendukung pembuktian dari kontrak jual beli tersebut. Terdapat beberapa keuntungan yang diperoleh oleh pembeli dan penjual dengan menggunakan internet sebagai media jual-beli, yaitu:

- Keuntungan bagi pembeli:
  a. Mengembangkan daya kompetisi penjual
  b. Menumbuhkan produktivitas pembeli
  c. Manajemen informasi yang lebih tepat
  d. Mengurangi biaya dan waktu dalam membeli barang
  e. Dapat melakukan perbandingan harga dengan mudah
- Keuntungan bagi penjual:
  a. Mengembangkan kesempatan dalam pengadaan barang atau jasa
  b. Meningkatkan efisiensi
  c. Dapat mengidentifikasi target pelanggan lebih tepat
  d. Mengurangi pengeluaran untuk biaya sewa toko dan pegawai

Dalam kehidupan, manusia secara tidak sadar telah bergantung pada kemajuan teknologi informasi, dari hal kecil hingga yang besar. Kemudahan dan kepraktisan yang ditawarkan oleh teknologi memunculkan berbagai kejahatan baru, oleh karena itu hukum harus ditingkatkan untuk perlindungan pengguna teknologi agar selalu merasa aman dan nyaman.[8] Seiring dengan perkembangan jaman dan perilaku masyarakat yang berubah mengikuti perubahan peradaban secara global, lahir suatu rezim hukum baru yang disebut dengan hukum siber yang merupakan hukum yang berhubungan dengan pemanfaatan teknologi informasi.

[8] Dony Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi* (Yogyakarta: Penerbit Andi, 2008), 421.

Meskipun *e-commerce* menawarkan kemudahan saat bertransaksi, ada satu masalah yaitu privasi. Menurut Zheng Qin dalam buku *Introduction to E-Commerce*, saat melakukan dan menerima transaksi daring maka harus memberikan data pribadi konsumen. Selain itu, jejak konsumen juga dapat dilacak dan dicatat tanpa sepengetahuan dari konsumen tersebut dan sementara pengumpul data bisa menjual informasi ini secara komersial ke organisasi lain. Maka dari itu apabila konsumen terlibat dalam *e-commerce* maka konsumen harus menyadari bahwa hal ini membuat privasi mereka tidak terlindungi.[9] Aktivitas ini dilakukan via jaringan sistem komputer dan internet hal ini dapat menyebabkan permasalahan hukum baru seperti cara penyampaian informasi, komunikasi, transaksi yang dilakukan via elektronik dan juga pembuktian yang berhubungan dengan perbuatan hukum yang dilakukan dari sistem elektronik.

Menurut Jonathan Rosenoer dalam bukunya, *CyberLaw: The Law of Internet* (1997), ruang lingkup *cyber law* meliputi:

- Hak Cipta (*Copyright)*
- Hak Dagang (*Trademark*)
- Pencemaran nama baik (*Defamation*)
- Ucapan Kebencian/Siar Kebencian (*Hate Speech*)
- Kejahatan Siber (*Cyber Crime*), antara lain seperti *Hacking*, *Viruses, Illegal Access*
- Privasi/Data Pribadi *(Privacy*)
- Kontrak Elektronik (*Electronic Contract*)
- Pornografi (*Pornography*)
- Perlindungan dalam kegiatan elektronik seperti *E-Commerce, E-Government*

Terdapat juga beberapa tindakan *cyber crime* yang sering dilakukan seperti:

- *Joy Computing*

  Terminologi di saat memakai komputer orang tanpa izin, yang termasuk pencurian waktu operasi komputer.
- *Hacking*

  Penggunaan teknologi termasuk komputer dengan cara yang tidak etis untuk menilai permasalahan komputer yang muncul. Terdapat beberapa jenis *hacking*, seperti:
- *Carding*

  Modus kejahatan transaksi daring yang menggunakan kartu kredit orang lain secara ilegal, dan pelaku mengetahui nomor kartu kredit korban yang diperoleh dari situs yang tidak

[9] Zheng Qin, *Introduction to E-Commerce* (Beijing: Tsinghua University Press, 2009), 194.

aman, atau membeli dari pencuri data. Sementara korban mengalami kerugian dan ditagih atas transaksi yang tidak pernah dilakukan. Terdapat beberapa cara untuk menghindari terjadinya *carding* yaitu dengan amati cara menggesek kartu saat transaksi *offline*, belanja di situs daring terpercaya, rahasiakan data pribadi khususnya nomor kartu kredit dan CVV, jangan fotokopi kartu kredit, saat bertransaksi/ belanja daring gunakan internet pribadi jangan terhubung dengan WIFI di tempat umum agar lebih aman.

- *Cyber-Pornography*

  Berasal dari dua kata, *cyber* dan *pornography,* kata *cyber* berasal dari kata *cybernetics* adalah bidang ilmu yang menggabungkan antara matematik, robotic, psikologi dan elektro atau yang lebih dikenal sebagai dunia maya. Menurut Kamus Besar Bahasa Indonesia, pornografi adalah penggambaran tingkah laku erotis dengan lukisan untuk membangkitkan nafsu birahi. Yang di mana dua kata tersebut disimpulkan sebagai pornografi dunia maya, yang merupakan penyebarluasan materi pornografi dalam dunia maya melalui teknologi informasi.

Maka dari itu pihak swasta maupun pemerintah mulai menyadari pentingnya perlindungan atas data pribadi. Salah satu contohnya adalah Kementerian Komunikasi dan Informatika (Kemkominfo) mengeluarkan kebijakan yang masih dalam bentuk Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang akan mengatur hak dan kewajiban pemilik data dan individu termasuk lembaga yang mengumpulkan dan memproses data. Nantinya regulasi ini yang akan menjadi pengawas perlindungan data pribadi sehingga perlindungan data pribadi diyakinkan aman.[10]

Meskipun Menteri Komunikasi dan Informatika telah mengeluarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik, di dalamnya hanya memuat secara terbatas ketentuan mengenai hak pemilik data pribadi, kewajiban pengguna data pribadi, penyelesaian sengketa dan kewajiban penyelenggara sistem elektronik. Undang-Undang Tentang Informasi dan Transaksi Elektronik (UU ITE) belum secara khusus memuat aturan perlindungan data pribadi, namun di Pasal 26 ayat (1) dan penjelasannya UU Nomor 19 Tahun 2016 menjelaskan bahwa selain yang ditentukan oleh perundang-undangan, informasi yang digunakan melalui media elektronik yang berhubungan dengan data pribadi seseorang harus memiliki persetujuan orang tersebut. Dalam menggunakan Teknologi Informasi, perlindungan data pribadi adalah bagian dari hak pribadi.

[10] Akbar Evandio, "Kominfo Harap RUU Perlindungan Data Pribadi Disahkan Awal 2021," *Bisnis ID*, 30 December 2020, https://teknologi.bisnis.com/read/20201230/101/1337114/kominfo-harap-ruu-perlindungan-data-pribadi-disahkan-awal-2021.

a. Hak pribadi adalah hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi adalah hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
c. Hak pribadi adalah hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Dalam kaitannya dengan data elektronik pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik telah mengatur bahwa data pribadi merupakan data mengenai seseorang yang telah teridentifikasi atau dapat diidentifikasi dengan sendiri atau dikombinasi dengan informasi lain melalui sistem elektronik ataupun non elektronik dengan secara langsung maupun tidak langsung.

Sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, perlindungan data pribadi merupakan salah satu hak asasi manusia yang perlu diberikan landasan hukum yang kuat untuk memberikan keamanan yang efektif dan memadai. Perlindungan data pribadi ditujukan untuk menjamin hak warga negara untuk melindungi diri pribadi serta menumbuhkan kesadaran masyarakat dalam menjamin pengakuan dan kehormatan atas krusialnya perlindungan atas data pribadi.

Sementara itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen belum secara khusus mengantisipasi kemajuan teknologi informasi. Namun dalam ruang lingkup internasional telah terdapat beberapa persetujuan yang dapat digunakan untuk melindungi konsumen dalam transaksi *e-commerce.* PBB adalah komisi yang menangani Hukum Perdagangan Internasional yang telah menyepakati *UNCITRAL Model Law on Electronic Commerce* dengan resolusi 51/162 sebagai contoh untuk kemajuan terhadap harmonisasi dan persatuan hukum perdagangan internasional terutama negara-negara yang berkembang.

Walaupun UNICTRAL *Model Law on Electronic Commerce* sudah diterapkan di beberapa negara akan tetapi tidak secara khusus menyebutkan perlindungan hukum terhadap konsumen. Peraturan tersebut secara tidak langsung dapat melindungi para pihak yang melakukan transaksi via *e-commerce.* Maka dari itu dapat melindungi konsumen yang menggunakan teknologi dalam transaksi jual beli di *e-commerce.*

Data pribadi berisiko disusupi dan dapat digunakan untuk melakukan penipuan melalui metode *phishing*, *spam* ataupun *malicious software* (*malware). Malware* telah menjadi ancaman bagi keamanan semua pengguna internet, baik organisasi ataupun individu. Estimasi menunjukkan bahwa komputer sering kali diinfeksi dengan virus, dan ada perkiraan sekitar

lima juta bot aktif di dunia (virus yang menyerang komputer). Sementara itu ada aktivitas kriminal yang melakukan serangan, terhadap internet penyedia, perusahaan *e-commerce* dan pengguna yang meninmbulkan efek *malware* yang menyikapi hal itu. Dunia terus melakukan pengembangan terhadap strategi untuk mengurangi ancaman dari luar. Penggunaan data pribadi secara ilegal adalah masalah besar dan krusial, hal ini dapat memunculkan berbagai pertanyaan mengenai bagaimana pengetahuan mengenai perlindungan hukum atau data pribadi pengguna *e-commerce* di Indonesia. Permasalahan ini berkaitan dengan aturan hukum yang berlaku dan kerja sama antara penegak hukum dan otoritas penegakan privasi, organisasi sektor swasta. Permasalahan ini mengingat bahwa Undang-Undang Perlindungan Data tidak diperuntukkan untuk menangani tindakan kriminal atas data pribadi.[11] Selain itu, perlu untuk dikaji perlindungan hukum bagi data pribadi pembeli.

B. Pembahasan

B.1 Analisis Perlindungan Hukum atas Data Pribadi Bagi Pengguna *E-Commerce* di Indonesia

Pasal 26 ayat (1) UU Nomor 19 Tahun 2016 tentang Informasi dan Layanan Elektronik menyatakan bahwa dalam semua informasi yang berhubungan via media elektronik wajib memiliki persetujuan orang yang bersangkutan. Setiap individu yang melakukan pelanggaran akan diajukan gugatan atas kerugian yang didapat dan orang pemilik data pribadi berhak untuk meminta Penyelenggara Sistem Elektronik untuk menghapus Informasi Elektronik yang ada di bawah kendali Penyelenggara Sistem Elektronik dan sudah tidak memiliki kepentingan lagi. Dalam peraturan ini, juga menyebutkan bahwa Penyelenggara Sistem Elektronik wajib menghapus informasi elektronik yang sudah tidak relevan lagi. Apabila setiap orang dengan sengaja atau tanpa hak melakukan perbuatan yang bertentangan dengan hukum untuk melakukan penyadapan atau pencurian data informasi elektronik dapat dikenakan penegakan hukum dari kepolisian, kejaksaan dan juga institusi lain yang memiliki wewenang.

Dalam Pasal 26 ayat (1) UU ITE, dijelaskan bahwa perlindungan data pribadi merupakan hak pribadi/*privacy rights.* Hak pribadi mencakup sebagai berikut:

a. Hak pribadi adalah hak untuk menjalankan kehidupan pribadi dan bebas dari gangguan.
b. Hak pribadi adalah hak untuk berkomunikasi dengan orang lain tanpa gangguan.

[11] "The OECD Privacy Framework," *Organisation for Economic Co-Operation and Development,* 2013, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, 92.

c. Hak pribadi adalah hak untuk menjaga akses informasi mengenai data dan kehidupan pribadi milik seseorang.

Tujuan dari kedudukan hukum dari pembeli di *E-Commerce* agar pembeli dapat memiliki hak penuh atas data pribadi mereka dan mengurangi kerugian yang disebabkan oleh pihak ketiga. Dalam pengaturan hukum menyesuaikan kepentingan perorangan dengan kepentingan masyarakat secara sebaik-baiknya dan berusaha untuk mencari keseimbangan antara memberikan kebebasan dan melindungi dari individu yang menyebabkan adanya interaksi yang akan menimbulkan konflik ataupun ketegangan antara kepentingan perorangan dan masyarakat.[12]

Pembahasan Studi Kasus Kebocoran Data di *E-Commerce*

Pada Mei 2020, Tokopedia mengalami kebocoran data pribadi, dimulai pada tanggal 2 Mei 2020, akun Whysodank mengunggah kumpulan data pribadi pengguna Tokopedia di sebuah forum *hacker* bernama RaidForums. Raidforums adalah forum yang digunakan oleh para *hacker* untuk melakukan transaksi jual beli file database yang telah diperoleh.[13] Peretas mengklaim telah memiliki 91 juta data pengguna Tokopedia yang telah diperoleh sejak bulan Maret 2020, kasus ini ditemukan oleh Under The Breach, sebuah perusahaan *cybersecurity* yang berasal dari Israel setelah menemukan hasil peretasan tersebut di RaidForums. Basis data tersebut dipasarkan Rp.74.300.000,- (tujuh puluh empat tiga ratus juta rupiah) dan memiliki kelengkapan data seperti nama jelas, email yang terdaftar, jenis kelamin, nomor ponsel, jumlah dan detil transaksi dan lainnya.[14] Setelah Tokopedia mengetahui hal ini, Tokopedia melaporkan kasus kebocoran data pengguna ke pihak kepolisian.

Pada 2 Mei 2020 malam hari, CEO Tokopedia William Tanuwijaya memberikan tanggapan dan mengkonfirmasi adanya kasus kebocoran data, pihaknya telah mengatasi kebocoran data mengikuti praktik terbaik (*best practice)* sesuai standar global dikarenakan Indonesia belum memiliki regulasi mengenai perlindungan data pribadi. *Best Practice* yang dilakukan seperti:

1. Pihak Tokopedia memberikan transparansi mengenai data apa yang bocor kepada para pengguna.

[12] Muhammad Ferdian, "Kedudukan Hukum Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis Terhadap Persaingan Usaha Tidak Jujur," *Jurnal Ilmiah Hukum Dirgantara* 9, no. 2 (2019), https://journal.universitassuryadarma.ac.id/index.php/jihd/article/view/355.
[13] Sorta Tobing, "Mengenal RaidForums, Forum Jacker Tempat Jual-Beli Data yang Bocor," *Katadata.co.id*, 6 May 2020, https://katadata.co.id/sortatobing/digital/5eb28857e2903/mengenal-raidforums-forum-hacker-tempat-jual-beli-data-yang-bocor.
[14] *Ibid.*

2. Pihak Tokopedia terus memberikan kabar mengenai perkembangan penanganan.
3. Pihak Tokopedia melakukan upaya perbaikan sistem internal.
4. Pihak Tokopedia bekerja sama dengan pemerintah dan pihak lain yang berwenang mengenai insiden kebocoran data yang terjadi.[15]

Pengaturan Layanan Platform *E-Commerce* dalam UU Informasi dan Transaksi Elektronik

Sejak lama dunia hukum telah melakukan perluasan terhadap asas dan norma untuk menghadapi persoalan benda yang tidak memiliki wujud, seperti kegiatan siber. Kegiatan siber sangat luas karena tidak memiliki batas dari negara dan dapat diakses dari mana saja dan kapan pun. Informasi elektronik belum terakomodasi dalam sistem hukum acara Indonesia dan sangat mudah untuk disadap, dipalsukan, diubah dan dikirim ke seluruh dunia dalam waktu yang sangat singkat. Dampak yang dihasilkan sangat luas dan rumit.

Permasalahan ini menjadi lebih kompleks ketika adanya *e-commerce* karena telah menjadi bagian dari ekonomi dunia. Hal ini membuktikan bahwa bidang telematika berkembang pesat, dalam kegiatan *e-commerce* atau adanya dokumen elektronik yang terdapat dokumen yang dibuat di atas kertas. Perlu diperhatikan keamanan dan kepastian hukum agar pengguna merasa aman dan dapat berkembang secara optimal. Dalam *cyber space,* perlu dilakukan pendekatan atas aspek hukum, teknologi, sosial, budaya dan etika. Untuk dapat menangani gangguan keamanan dalam PSE maka harus dilakukan pendekatan hukum yang mutlak karena tanpa adanya kepastian hukum permasalahan pemanfaatan teknologi menjadi tidak optimal.[16]

Pengaturan Data Privasi di Hong Kong, Korea Selatan dan Malaysia

Pengaturan Data Privasi di Hong Kong

Personal Data Privacy Ordinance of 1995 (PDPO) Hong Kong adalah peraturan perundang-undangan yang mengatur pertama kali mengenai masalah privasi data secara komprehensif di Asia. Pada tahun 1997, setelah Hong Kong menggabungkan kembali pada Republik Rakyat Cina, Hong Kong dan Macau menjadi satu-satunya regional di Cina yang

[15] Fahmi Ahmad Burhan, "Tokopedia Ungkap Cara Atasi Kasus Kebocoran Data Pribadi," *Katadata.co.id*, 15 September 2021, https://katadata.co.id/lavinda/digital/61421ec0427f1/tokopedia-ungkap-cara-atasi-kasus-kebocoran-data-pribadi.
[16] *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

memiliki hukum privasi data yang cakupannya luas. Setelah 18 tahun terdapat implementasi oleh *Privacy Commissioner for Personal Data* (PCPD), otoritas Hong Kong yang bertanggung jawab untuk masalah privasi, prinsip perlindungan privasi dalam PDPO tidak dapat dijalankan. Maka pada tahun 2012, terdapat perubahan besar dalam PDPO.[17]

Di Hong Kong, PDPO dibuat berdasarkan adanya pendapat dari para elit politik pemerintah kolonial di Hong Kong bukan karena tuntutan masyarakat atau permasalahan yang dihadapi. Pada tahun 1995, proses pengesahan PDPO adalah antisipasi kemajuan di Eropa yang memiliki pengaruh terhadap hubungan perdagangan terhadap Hong Kong. Pada dasarnya, PDPO adalah undang-undang yang memiliki hubungan terhadap perlindungan hak asasi manusia. Karena adanya PDPO, pemerintah Hong Kong menganggap bahwa nilai ekonomi akan terus bertambah dan memiliki jaminan kelancaran perpindahan data privasi ke Hong Kong.[18]

Komisi Privasi untuk perlindungan memberikan amanat untuk membangun Komisioner Privasi Data privasi sebagai suatu badan independen yang memiliki fungsi untuk mengawasi dan menyosialisasikan agar masyarakat patuh terhadap PDPO dan juga memberikan penjelasan terhadap masyarakat terhadap PDPO, memeriksa legislasi yang diajukan agar pemberlakuan legislasi tidak akan memengaruhi privasi individual tetapi menjalankan pemeriksaan sistem pengelolaan data privasi dan memiliki penelitian dalam bidang PDPO. [19]

Pengaturan Data Privasi di Korea Selatan

Sejak 1980, Korea merupakan demokrasi multipartai dan adalah negara yang memiliki hukum yang kuat. Dalam perlindungan data privasi, pada tahun 2011 Korea Selatan mempunyai *Personal Information Protection Act* (PIPA). Dalam PIPA terdapat cakupan yang komprehensif dan memiliki prinsip perlindungan yang inovatif dan PIPA membuat dimungkinkannya Korea Selatan memiliki cara penegakan perlindungan privasi yang kuat.[20]

Salah satu faktor yang membentuk kaidah di dalam PIPA adalah tingginya pengguna internet di Korea Selatan. Sekitar 80% populasi Korea adalah pengguna internet, hal ini dikarenakan Korea Selatan memiliki konektivitas *broadbrand* tertinggi kedua di antara negara OECD. Karena tingginya angka pengguna internet, maka Korea Selatan menyetujui untuk

[17] Shinta Dewi, *Op. Cit.*, 65.
[18] *Ibid.,* 66.
[19] *Ibid.*
[20] *Ibid.,* 73.

mengesahkan beberapa regulasi untuk penggunaan internet dan aturan yang memiliki hubungan implikasi terhadap data privasi. Konstitusi Korea memberikan perlindungan umum terhadap privasi di tempat tinggal serta dalam berkomunikasi dan juga mengeraskan kalau hak warga negara dan kebebasan tidak dapat didiamkan dengan alasan kalau hak tersebut tidak ada dalam konstitusi tetapi dapat dikecualikan apabila menyangkut keamanan nasional, hukum dan ketertiban ataupun kesejahteraan umum.[21]

PIPA bertanggung jawab atas perlindungan data privasi di publik atau swasta dan dalam Pasal 2 PIPA menjelaskan bahwa data pribadi merupakan informasi yang dimiliki oleh manusia yang dapat mengidentifikasi individu tersebut dari nama atau NIK, gambar dan lain-lain. Hal ini dapat digunakan dengan mengombinasikan beberapa data untuk membantu mengidentifikasi seseorang. Dalam Pasal 3 dan 4, Legislasi Korea Selatan membuat ketentuan untuk dapat membatasi pengumpulan data privasi, persetujuan dan pemberitahuan. Pengolahan data privasi wajib menjelaskan secara detil dan eksplisit maksud dan tujuan pengolahan data privasi.[22]

Pengaturan Data Pribadi di Malaysia

Sejak tahun 1998, Menteri Malaysia telah menyusun rencana untuk membentuk undang-undang perlindungan data yang lengkap. Hingga pada tahun 2010, Malaysia mengesahkan Undang-Undang Perlindungan Data Privasi atau yang dikenal dengan *Personal Data Protection Act* (PDPA) 2010. Setelah itu pemerintahan Malaysia membuat Departemen Perlindungan Data Privasi yang menjadi tanggung jawab Kementerian Informasi Komunikasi dan Kebudayaan yang berhak atas pelaksanaan PDPA 2010.[23]

Dijelaskan dalam Pasal 5 ayat (1) bahwa tidak ada orang yang akan dirampas kebebasan pribadinya kecuali sesuai dengan hukum, mengenai ketentuan ini Pengadilan Federal Malaysia menjabarkan bahwa dalam Pasal 5 ayat (1) termasuk hak lain yang salah satunya adalah hak privasi. Pada sisi lainnya, Malaysia belum mengesahkan *International Covenant Civil and Political Rights* (ICCPR) 1996 maka dari itu tidak mengikuti kewajiban yang berdasar pada perjanjian internasional mengenai privasi. Tetapi Malaysia adalah anggota dari *Asia Pacific Economic Cooperation* (APEC) dan mematuhi kerangka privasi dari APEC yaitu APEC

[21] *Ibid.,* 74.
[22] *Ibid.,* 75.
[23] *Ibid.,* 77.

Privacy Framework, akan tetapi Malaysia tidak dapat pihak yang dalam Aturan Privasi Lintas Batas atau *APEC Crossborder Privacy Rules/CBPR.*[24]

Terdapat 7 (tujuh) prinsip Perlindungan Data Privasi yang disebutkan dalam PDPA 2011 yaitu:[25]

a. Prinsip Umum – Pengolahan Berdasarkan Persetujuan

   Dalam seksi 6 PDPA terdapat aturan prinsip umum bahwa pengguna data dapat memproses data privasi apabila subjek data telah memberikan persetujuan. Pengolahan data termasuk dari proses pengumpulan, penyimpanan, penggunaan dan pengungkapan hingga penghancuran.

b. Keabsahan, Kebutuhan dan Tidak Berlebihan

   Dalam seksi 6 ayat 3 PDPA menyebutkan tiga batas umum pada pengolahan data privasi yang berdasarkan dari tujuan seperti:

   a. Pengolahan data harus dilakukan apabila memiliki tujuan yang sah dan memiliki hubungan langsung dengan kegiatan dari pengguna data.
   b. Pelaksanaan pengolahan data harus serentak yang dibutuhkan dengan tujuan dari pengolahan data.
   c. Data privasi yang diolah harus mencapai tujuan pengolahan tetapi tidak berlebihan.

c. Prinsip Pengumpulan dan Pemberitahuan

   Pengguna data wajib memberikan pemberitahuan tertulis bahwa data tersebut digunakan dan harus dengan secepat mungkin ketika data yang dikumpulkan dari subjek data harus dengan pemberitahuan tertulis.

d. Prinsip Penggunaan dan Pengungkapan

   Penggunaan data privasi dalam seksi 6 ayat (3) memberi syarat bahwa data privasi tidak dapat diproses hanya kalau data privasi memiliki tujuan yang sah dan memiliki hubungan dengan aktivitas pengguna data dan pengolahan data privasi memiliki tujuan dengan pengumpulan data privasi.

e. Data Privasi Sensitif

   Data privasi sensitif juga meliputi kesehatan/kondisi fisik, agama, keyakinan, pilihan politik dan data lainnya yang telah ditentukan oleh Menteri sebagai data privasi sensitif. Data privasi merupakan informasi mengenai transaksi komersial, hal ini yang membatasi lingkup perlindungan data privasi sensitif.

[24] *Ibid.*
[25] *Ibid.*

Untuk dapat melakukan pengolahan data privasi diperlukan persetujuan eksplisit, pengolahan data privasi juga dapat dilakukan tanpa persetujuan apabila pihak pengolahan ada di dalam kategori pengecualian. Dalam hal ini, yang ada dalam kategori pengecualian adalah pengolahan data yang diproses untuk dapat menjalankan fungsi yang diberikan kepada setiap individu dan berdasarkan undang-undang atau memiliki tujuan lain yang telah ditetapkan oleh Menteri yang bertanggung jawab. Selain itu ada pengecualian apabila individu tersebut telah dengan sendirinya tanpa paksaan mempublikasi data privasi sensitif mereka sendiri, akan tetapi hal ini menimbulkan kekhawatiran karena akan disalahkan oleh Malaysia.

f. Prinsip Keamanan

Dalam prinsip ini, mewajibkan para pengguna data untuk mengambil langkah yang dapat diterapkan untuk memenuhi enam faktor keamanan. Dalam seksi 6 *Personal Data Protection Regulations* memerlukan para pengguna data untuk mempunyai kebijakan keamanan yang telah dirasa sesuai dengan standar keamanan yang ditetapkan secara teratur.

g. Prinsip retensi data dan hak untuk memblokir pemrosesan

Setelah mencapai tujuan, data privasi tidak boleh disimpan lebih lama lagi. Pengguna data harus bertanggung jawab untuk data privasi tersebut dihancurkan. Pengguna data harus mengikuti retensi standar yang menerapkan Komisioner perlindungan data privasi.

Berdasarkan seksi 38 PDPA dapat memperoleh persetujuan untuk mematuhi pengolahan data setiap saat. Selain itu, hak untuk menarik izin pengolahan juga sangat penting dalam praktik pemasaran langsung. Subjek data mempunyai hak untuk memilih keluar dari penggunaan pemasaran langsung kapan saja di luar dari persetujuan yang telah diberikan.

h. Prinsip Integritas Data

Bagi pengguna data harus memilih langkah yang terbaik untuk dapat menjamin bahwa data privasi tersebut akurat lengkap, ter-*update* dan memiliki tujuan.

i. Prinsip Akses dan Koreksi

Untuk mengakses data privasi mereka, subjek data memiliki hak standar untuk dapat melakukan modifikasi terhadap data apabila tidak akurat, tidak lengkap, dan data tersebut salah. Dalam *Personal Data Protection Regulations 2013,* telah menentukan bahwa subjek data dapat melakukan perubahan terhadap data kecuali Komisioner Perlindungan Data Privasi berkata lain.

B.2 Analisis Perlindungan Hukum Data Pribadi Pembeli di *E-Commerce* di Indonesia

Dalam *e-commerce* wajib ada perlindungan atas informasi pribadi (*personal data).* Segala bentuk transaksi di *e-commerce* harus dilindungi dari subjek data yang sesuai dengan prinsip dan norma etika yang ada.[26] *Privacy Policy* adalah tanggung jawab dan pelaksanaan untuk melindungi hak privasi seorang individu yang telah memberikan data privasinya pada saat mendaftarkan dirinya dalam kegiatan *e-commerce.*

Dalam setiap transaksi *e-commerce*, *privacy policy* dapat diakses dalam setiap transaksi dengan mudah karena menjadi sangat penting dalam kegiatan jual beli daring dan menjadi *code of conduct* yang dihormati oleh semua pihak.[27] Dalam peraturan hukum memberi penjelasan secara menyeluruh tentang kewajiban dan tanggung jawab dari penjual/pelaku usaha mengenai proteksi pada status perlindungan konsumen yang baik dan memberlakukan prinsip *favourable. Favourable* merupakan pernyataan yang bersifat positif yang memberi dukungan aspek dalam variabel. Terdapat integrasi *standard privacy policy* yang terdapat dalam *online marketplace system online marketplace system* yang ada dicocokkan dalam Pasal 2 *Distance Contract Act*, yang di mana memastikan bahwa penyedia jasa *e-commerce* dan konsumen memiliki hubungan dan perikatan baik dan menjamin bahwa adanya perlindungan atas data privasi.

Terdapat dua jalan hukum yang ditempuh oleh konsumen apabila terjadi pelanggaran data privasi yaitu proses ajudikatif (litigasi dan arbitrase) dan proses konsensus (mediasi dan negosiasi). UNCTAD dalam *e-commerce and development report 2003* memberikan unsur untuk penyelesaian unsur dalam proses ajudikatif dan konsensus yang memiliki hubungan dengan hukum yang ada bagi yang melakukan pelanggaran yang sesuai dengan UU Nomor 11 Tahun 2008 tentang ITE dan PP Nomor 71 Tahun 2019 tentang PSTE yang di mana korban dapat melakukan gugatan kerugian perdata (menuntut atas ganti rugi).

Dalam kegiatan *e-commerce* membuktikan bahwa konsumen adalah pihak yang lemah dalam setiap transaksi, di mana terdapat aturan teknis yang berhubungan dengan *code of conduct* dari aktivitas *e-commerce* bahwa dapat memberi perlindungan terhadap kepentingan konsumen via detail per-consent dari *privacy policy* yang ada di dalam setiap transaksi yang telah disetujui oleh kedua pihak hingga PSE tidak dapat mengumpulkan data untuk keuntungan mereka sendiri. Pihak penengah menjadi pihak yang memberikan kontrol atas *privacy policy*

[26] Ida Bagus Rahmadi Supancana, *Cyber Ethics dan Cyber Law* (Jakarta: Penerbit Universitas Katolik Indonesia Atma Jaya, 2020), 47.
[27] Jovan Kurbalija, *An Introduction to Internet Governance* (Geneva: Diplo Foundation, 2016), 6.

dan disetujui oleh penyedia jasa dengan konsumen yang berhubungan dengan privasi data konsumen yang dilakukan secara daring.

Di hukum Indonesia terdapat Undang-Undang No. 11 Tahun 2008 tentang Informasi & Transaksi Elektronik (ITE), UU ini dapat bantu membahas beberapa permasalahan misalnya pengakuan terhadap suatu transaksi atau dokumen elektronik dalam hukum perdata Indonesia dalam hukum pembuktian dan hukum perikatan sehingga kepastian hukum transaksi elektronik aman. Dalam UU ITE juga menyebutkan beberapa klasifikasi tindakan yang termasuk dalam pelanggaran hukum yang berhubungan dengan penyalahgunaan teknologi informasi dan ada sanksi pidana.

Sebelum lahirnya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang yang mengatur kegiatan yang memiliki hubungan dengan *e-commerce* diatur di beberapa peraturan undang-undang seperti Undang-Undang No. 12 Tahun 2002 tentang Hak Cipta, Undang-Undang No. 15 Tahun 2001 tentang Merek, Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, serta Undang-Undang No. 14 Tahun 2001 tentang Paten.

Namun hingga saat ini, walaupun transaksi *e-commerce* terus meningkat, Indonesia belum memiliki regulasi atau perundang-undangan mengenai perlindungan data pribadi. Belum ada pengaturan yang khusus membahas perlindungan data pribadi untuk pengguna *e-commerce* hanya menjelaskan aspek perlindungan data pribadi secara luas.

Kajian Akademik Terhadap UU Perlindungan Data Pribadi

Berikut adalah beberapa materi muatan yang diatur dalam RUU Perlindungan Data Pribadi yang perlu dikaji:

1. **Dimuatnya Asas-Asas di Bidang Hukum Perlindungan Data Pribadi dalam Pertimbangan dan Pasal-Pasalnya**

   Asas perlindungan merupakan dasar dari perlindungan data pribadi dan sebagai asas kepentingan umum yang menjadi pengecualian dapat diterobosnya data pribadi dan asas keseimbangan yang mengatur batasan antara hak individu, negara dan asas pertanggungjawaban yang menjadi landasan bagi pelaku usaha untuk menjalankan sistem pemrosesan, penyebarluasan, pengelolaan dan pengawasan data pribadi yang memberikan dasar bagi pasal yang merincikan perlindungan data pribadi.

2. Kesepakatan dari Konsumen untuk Menyerahkan Data Pribadi pada Pelaku Usaha dan Keterbukaan Informasi terhadap Penyimpanan dan Pengolahan Data oleh Pelaku Usaha

Sebelum konsumen menyerahkan data, yang harus dilakukan pertama adalah kesepakatan (*consent*) dari para pihak yang memiliki keterkaitan dalam proses penyerahan data. Untuk dapat memenuhi asas konsensualitas dalam segala perikatan diperlukan bentuk pengaturan tentang materi muatan yang terpenting. Kesepakatan dapat dibuat dalam bentuk tertulis, serta eksplisit dan terdapat tanda tangan ataupun tanda tangan digital yang menjadi bukti bahwa konsumen telah dengan sadar menyetujui data pribadi diproses oleh pelaku usaha. Dalam hal ini, dapat mempermudah untuk melakukan pembuktian apabila terjadi konflik yang berujung dengan sengketa.[28] Kesepakatan juga harus mencakup secara jelas tujuan dari penggunaan data pribadi yang dikumpulkan agar hanya diperbolehkan sebatas dengan tujuan yang telah disepakati bersama.

3. Hak-hak Pemilik Data Pribadi

Hak Pemilik data pribadi perlu dijelaskan secara rinci, sebagai berikut:

a) Hak untuk mengajukan akses yang memadai
b) Hak atas salinan data pribadi dari pengelola data pribadi
c) Hak meminta pengelola data untuk memperbaiki kesalahan yang terdapat pada data pribadi yang sebelumnya telah diberikan dan tersimpan
d) Hak untuk memperbaharui data pribadi yang berada pada pengelola data
e) Hak untuk melengkapi data dan pribadi sebelum data pribadi tersebut dikelola oleh pengelola
f) Hak untuk meminta pada pengelola data pribadi untuk memusnahkan data pribadi konsumen
g) Hak untuk menuntut dan menerima ganti rugi atas pelanggaran terhadap hak konsumen
h) Hak untuk dapat setiap saat menarik kembali persetujuan pengelolaan data yang telah diberikan
i) Hak untuk dapat setiap saat menarik kembali persetujuan pengelolaan data yang telah diberikan pada pengelola data dengan pemberitahuan

[28] Ana Sofa Yuking, "Urgensi Peraturan Perlindungan Data Pribadi dalam Era Bisnis Fintech," *Jurnal Hukum & Pasar Modal* 3, no. 16 (2018).

Penyimpanan data dan akses terhadap data tersebut sudah seharusnya dijamin agar seseorang dapat menjalankan hak untuk mendapatkan pengamanan data miliknya dan untuk mengkoreksi data apabila ada kesalahan pada data yang disimpan.

4. Perbedaan Antara Data Pribadi dan Data Pribadi Sensitif

Dalam RUU Perlindungan Data Pribadi (tahun 2015), pengertian data pribadi adalah "setiap data tentang kehidupan seseorang baik yang teridentifikasi dan/atau diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik." Namun dalam RUU PDP membedakan antara data pribadi dan data pribadi sensitif. Setelah melakukan pemrosesan data setelah itu terdapat pembedaan tingkat perlindungan data pribadi sensitif dan perlindungan tingkat tinggi.

5. Kewajiban Pelaku Usaha Bagi Aktivitas yang Berkaitan dengan Pengumpulan, Pengendalian, Pemrosesan dan Penggunaan Data Pribadi

Pihak pengelola data pribadi juga adalah badan hukum maka perlu mengatur mengenai kewajiban yang menjadi beban tanggung jawab pelaku usaha dalam memberikan jasa dan mengumpulkan dan proses data. Kewajiban lain yang terdapat dalam RUU PDP adalah:

a) Legalitas dari pengelola data pribadi
b) Kejelasan tujuan pengelolaan data pribadi
c) Jenis-jenis data pribadi harus diklasifikasikan
d) Perincian periode retensi dokumen yang memuat data pribadi termasuk jangka waktu pengelolaan dan pemusnahan data
e) Perincian keterangan data pribadi yang dikumpulkan
f) Kewajiban untuk tidak mencegah atau mempersulit pemilik data untuk merubah, menghapus, dan menarik kembali data pribadinya untuk dikelola penyelenggara jasa
g) Kewajiban untuk menunda proses pengelolaan data pribadi sebagian atau seluruhnya apabila dimintakan penundaan oleh pemilik data
h) Pengumuman kebijakan penggunaan privasi bagi konsumen dan/atau calon konsumen
i) Pemenuhan hak yang berkaitan dengan habeas data pada bagian sebelumnya selaku kewajiban penyelenggara jasa
j) Memastikan pengawasan optimal terhadap tenaga kerja yang terlibat dalam pengelolaan data pribadi
k) Memastikan bahwa data pribadi adalah akurat dan lengkap apabila data tersebut akan dimintakan untuk membuat suatu keputusan yang mempengaruhi pemilik data pribadi (contoh riwayat penyakit atau catatan medis dalam bentuk lainnya)

l) Memastikan keamanan sistem agar tidak terbobol dan terjadi pencurian data
m) Bertanggung jawab atas segala kelalaian atau kesengajaan yang menimbulkan tidak terpenuhinya perlindungan data pribadi konsumen
n) Kewajiban untuk memusnahkan data pribadi apabila: telah mencapai periode retensi; tujuan pengelolaan data pribadi telah tercapai; atau terdapat permintaan dari pemilik data
o) Kewajiban untuk melakukan pemberitahuan pada pemilik data yang dirugikan tanpa penundaan fakta bahwa data pribadi miliknya terungkap
p) Kewajiban untuk menginformasikan pemasangan alat pemroses data visual ke masyarakat dan menjamin keamanan data pribadi yang diperolehnya dari alat pemroses data visual (seperti perekaman biometrik)

Maka apabila kedepannya terjadi pembobolan data atau terlibat dalam perbuatan tindak pidana korupsi, analisis konsumen tanpa persetujuan konsumen, penipuan, pencucian uang, pendanaan terorisme, dan penggelapan yang dengan sengaja dilakukan atau dibiarkan oleh pelaku usaha maka pelaku usaha dapat dijerat. Dalam Pasal 6, menyatakan bahwa data harus diproses secara adil dan berdasarkan hukum, pengumpulan data harus spesifik dan jelas, dan tujuannya dapat disahkan oleh hukum. Apabila terjadi pelanggaran, maka orang yang merasa dirugikan dapat meminta pertanggungjawaban dan ganti rugi pada negara.[29]

6. Pemenuhan Privasi dan Perlindungan Data Pribadi sebagai HAM

Perlindungan data pribadi adalah suatu pengakuan, perlindungan dan pemenuhan HAM yang harus ada di dalam RUU. Hukum positif yang ada harus memberikan perlindungan terhadap hidup dan barang seseorang, karena data pribadi telah dinilai sebagai barang berharga dan tidak berwujud. Maka dari itu apabila terjadi pelanggaran hukum terhadap data pribadi maka orang yang merasa dirugikan dalam menuntut ganti rugi pelanggaran hukum tersebut.

7. Pembentukan Komisi Pengawas

Pembentukan komisi diperlukan untuk memastikan efektivitas dari RUU PDP. Tugas dari komisi untuk memantau kepatuhan semua pihak yang terkait dengan pengumpulan data pribadi dan juga berperan dalam memberikan arahan bagi penyelenggara jasa untuk memenuhi standar minimum dalam PDP, menerima pengaduan, memfasilitasi penyelesaian sengketa dan melakukan pendampingan terhadap pemilik data apabila terjadi pelanggaran.

[29] European Commission, *Ethics and Data Protection 14 November 2018.*

Komisi pengawas dituntut agar mampu merumuskan dan melaksanakan rencana dan kebijakan untuk memperkuat perlindungan data pribadi dan mempublikasikan dengan cara terorganisir panduan dan langkah-langkah perlindungan data pribadi untuk memberi rekomendasi pada aparat penegakan hukum dalam hal penuntutan yang memiliki hubungan dengan PDP seperti melakukan penelitian, memberikan surat teguran pada pihak pengelola data pribadi, melakukan penelitian dan memberikan saran dan pendapat bagi penerapan peraturan yang memiliki hubungan dengan PDP dan melakukan kerja sama dengan otoritas negara lain serta membentuk sekretariat untuk mempermudah pelaksanaan UU PDP dan lainnya.

8. **Pemberian Sanksi bagi Pelanggar**

   Pelanggaran yang memiliki keterkaitan dengan hak atas data pribadi harus diberikan untuk memberikan kepatuhan, edukasi dan juga penyesalan. Dalam komparatif, hukuman penjara dan denda untuk kasus pencurian data sudah diterapkan di negara seperti Korea Selatan, Hong Kong, Singapura dan Malaysia. Hukuman yang diberikan juga harus sesuai dengan pelanggaran yang dilakukan, sanksi yang diberikan adalah sanksi pidana dan juga administratif. Pemberian sanksi juga harus disesuaikan dengan ketentuan peraturan perundang-undangan yang telah berlaku.

9. **Partisipasi Masyarakat sebagai Unsur Pendukung Pelaksanaan Perlindungan Data Pribadi**

   Agar dapat memperlancar penyelenggaraan dari PDP maka harus diberikan Pendidikan ataupun pelatihan dan advokasi, bimbingan dan sosialisasi melalui media ataupun seminar untuk masyarakat.

Perbandingan Hukum Data Pribadi di Hong Kong, Korea Selatan, Malaysia dan Indonesia

Hong Kong memiliki *Personal Data Privacy Ordinance of 1995* (PDPO) Hong Kong adalah peraturan perundang-undangan yang mengatur pertama kali mengenai masalah privasi data secara komprehensif di Asia. Lalu pada tahun 2012, Hong Kong melakukan perubahan terhadap PDPO 1995 karena belum seluruh prinsip yang terdapat dalam PDPO tahun 1995 masih mengalami kekurangan.

Korea Selatan merupakan salah satu negara yang memiliki aturan hukum yang terbaik dan terdepan, pada tahun 2011 Korea memiliki aturan *Personal Information Protection Act* (PIPA). Konstitusi Korea memberikan perlindungan untuk privasi yang meliputi perlindungan privasi di tempat tinggal dan juga dalam berkomunikasi.

Malaysia memiliki peraturan perundang-undangan *The Personal Data Protection Act* No. 709 of 2010 (PDPA Malaysia) untuk memberikan perlindungan terhadap data pribadi. Sejak tahun 1998, Menteri Malaysia telah melakukan perencanaan pembentukan UU PDP, dan akhirnya di tahun 2010 PDPA Malaysia telah disahkan.

Undang-Undang Perlindungan Data Pribadi Indonesia sampai saat ini masih dalam bentuk rancangan yang belum disahkan dan diundangkan. Akan tetapi Indonesia memiliki beberapa peraturan yang memiliki keterkaitan dengan perlindungan data pribadi seperti:

a. Undang-Undang No. 10 Tahun 1998 tentang Perbankan
b. Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi
c. Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen
d. Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia

Di antara 4 negara di Asia yang telah dibahas, Korea Selatan, Hong Kong, Malaysia dan Indonesia, dijadikan perbandingan dengan negara Indonesia dikarenakan masih dalam Asia Tenggara dan memiliki peraturan dan hukum yang kurang lebih sama dan tingkat pengguna internet yang hampir sama. Hong Kong Korea Selatan dan Malaysia adalah negara yang telah menerapkan peraturan untuk Perlindungan Data Pribadi dan juga memberikan saksi pidana ataupun administratif bagi siapapun yang melanggar. Namun, dalam hal ini Korea Selatan memiliki Undang-Undang Perlindungan Data Pribadi terdepan dan memiliki perlindungan privasi untuk rumah tinggal dan komunikasi. Hong Kong merupakan salah satu negara di Asia yang memiliki Undang-Undang Perlindungan Data Pribadi pertama, karena menurut Menteri Hong Kong, apabila Hong Kong memiliki UU PDP maka akan membuat ekonomi Hong Kong berkembang dan mengundang investor internasional. Malaysia merupakan salah satu negara yang memiliki rancangan undang-undang sejak tahun 1998 dan baru disahkan tahun 2010, dapat disimpulkan bahwa banyaknya pertimbangan yang diambil untuk menyempurnakan undang-undang tersebut.

Indonesia sampai saat ini masih dalam proses Rancangan Undang-Undang Perlindungan Data Pribadi maka diharapkan agar Undang-Undang Perlindungan Data Pribadi tersebut dapat segera disahkan. Namun menurut Penulis bahwa Rancangan Undang Undang Perlindungan Data Pribadi sudah cukup jelas dan lengkap memenuhi aspek perlindungan data pribadi.

C. Kesimpulan

Berdasarkan pembahasan dan analisis dalam bagian sebelumnya dapat disimpulkan sebagai berikut:

1. Saat ini Indonesia masih belum memiliki undang-undang yang mengatur mengenai perlindungan data pribadi dalam *e-commerce.* Walaupun dalam sehari-hari penggunaan *e-commerce* semakin meningkat namun belum ada aturan hukum yang mendasarinya, terutama untuk memberikan jaminan perlindungan bagi konsumen, data pribadi dan kenyamanan internet. Perkembangan *e-commerce* di Indonesia terhambat karena teknologi dan infrastruktur yang terbatas, keamanan, undang-undang dan juga sumber daya manusia. Kedudukan hukum mengenai perlindungan data pribadi dan *e-commerce* masih merujuk pada Undang-Undang No. 11 Tahun 2008 terhadap Informasi dan Transaksi Elektronik (ITE). UU ITE dapat menyelesaikan dan menjelaskan secara umum permasalahan yang berhubungan dengan transaksi elektronik dan dokumen elektronik.
2. Di Indonesia, peraturan mengenai perlindungan data pribadi masih dalam bentuk rancangan dan belum disahkan sampai saat ini maka sering kebocoran data pribadi yang tidak mendapatkan penyelesaian secara hukum. Hal ini, membuktikan bahwa masyarakat Indonesia masih kurang memiliki kesadaran atas betapa penting data pribadi mereka. Oleh karena itu, masyarakat harus diberikan edukasi atas pentingnya perlindungan data pribadi dan harus lebih berhati-hati saat mengumpulkan data pribadi ke suatu aplikasi/*website*. Masyarakat perlu membaca *terms and conditions* pada saat mengumpulkan data pribadi mereka. Apabila dilakukan perbandingan dengan negara lain di Asia, RUU PDP dinilai sudah cukup baik karena telah mengatur aspek dari pihak-pihak pengelola data, pengguna dan pihak ketiga.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Buku

Ariyus, Dony. *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Yogyakarta: Penerbit Andi, 2008.

Dewi, Shinta. *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional.* Bandung: Widya Padjajaran, 2009.

European Commission. *Ethics and Data Protection 14 November 2018*.

Kurbalija, Jovan. *An Introduction to Internet Governance.* Geneva: Diplo Foundation, 2016.

Qin, Zheng. *Introduction to E-Commerce*. Beijing: Tsinghua University Press, 2009.

Rosenoer, Jonathan. *CyberLaw: The Law of Internet.* New York: Springer, 1997.

Supancana, Ida Bagus Rahmadi. *Cyber Ethics dan Cyber Law.* Jakarta: Penerbit Universitas Katolik Indonesia Atma Jaya, 2020.

Jurnal Ilmiah

Ferdian, Muhammad. "Kedudukan Hukum Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis Terhadap Persaingan Usaha Tidak Jujur." *Jurnal Ilmiah Hukum Dirgantara* 9, no. 2 (2019): 74–96. https://journal.universitassuryadarma.ac.id/index.php/jihd/article/view/355.

Yuking, Ana Sofa. "Urgensi Peraturan Perlindungan Data Pribadi dalam Era Bisnis Fintech." *Jurnal Hukum & Pasar Modal* 3, no. 16 (2018): 1–27.

Media Internet

Bank Indonesia. "Pertumbuhan Ekonomi Indonesia Triwulan IV 2020." 5 February 2021. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_233321.aspx.

Burhan, Fahmi Ahmad. "Tokopedia Ungkap Cara Atasi Kasus Kebocoran Data Pribadi." *Katadata.co.id*, 15 September 2021. https://katadata.co.id/lavinda/digital/61421ec0427f1/tokopedia-ungkap-cara-atasi-kasus-kebocoran-data-pribadi.

Evandio, Akbar. "Kominfo Harap RUU Perlindungan Data Pribadi Disahkan Awal 2021." *Bisnis ID*, 30 December 2020. https://teknologi.bisnis.com/read/20201230/101/1337114/kominfo-harap-ruu-perlindungan-data-pribadi-disahkan-awal-2021.

Organisation for Economic Co-Operation and Development. "The OECD Privacy Framework." 2013. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Sirclo. "Menilik Tren Perkembangan E-Commerce Indonesia di 2020." Last modified 19 August 2020. https://www.sirclo.com/blog/menilik-tren-perkembangan-e-commerce-indonesia-di-2020/.

Tobing, Sorta. "Mengenal RaidForums, Forum Jacker Tempat Jual-Beli Data yang Bocor." *Katadata.co.id*, 6 May 2020. https://katadata.co.id/sortatobing/digital/5eb28857e2903/mengenal-raidforums-forum-hacker-tempat-jual-beli-data-yang-bocor.