



PERLINDUNGAN DATA PRIBADI DI INDONESIA DALAM RANGKA PERDAGANGAN ELEKTRONIK (*E-COMMERCE*)

Nanami Satyanegara*, Joko Priyono, Darminto Hartono Paulus
Program Studi S1 Ilmu Hukum, Fakultas Hukum Universitas Diponegoro
Email: nanami.sn1@gmail.com

Abstrak

Sekarang ini, dunia telah memasuki masa revolusi industri 4.0. Salah satu unsur revolusi industri 4.0 adalah *Big Data*, yang merupakan masa terjadinya pengumpulan dan pengolahan segala jenis data, termasuk data pribadi. Perkembangan teknologi menyebabkan terjadi banyak perubahan dalam kehidupan masyarakat, salah satunya adalah transaksi secara elektronik (*e-commerce*). Sebelum menggunakan jasa *e-commerce*, pengguna jasa harus memasukkan data pribadi. Namun setelah memasukkan data, konsumen tidak mengetahui cara penyimpanan dan pengelolaan data tersebut diproses. Hal ini menyebabkan kerentanan terjadinya penyalahgunaan data pribadi oleh perusahaan maupun pihak lainnya. Metode yang digunakan dalam penulisan hukum ini adalah metode penelitian yuridis normatif dengan spesifikasi penelitian deskriptif analitis. Penelitian ini menggunakan data sekunder yang diperoleh dari studi kepustakaan data hukum primer, sekunder dan tersier. Data yang terkumpul diolah dan dianalisis dengan metode analisis kualitatif. Hasil penelitian dapat disimpulkan bahwa data pribadi merupakan hak seseorang yang harus dilindungi dan hal ini telah diatur dalam konstitusi negara Indonesia, Undang-undang Dasar Negara Republik Indonesia tahun 1945. Dengan demikian, perusahaan *e-commerce* dalam menyimpan dan mengelola data pribadi harus memperhatikan hak pengguna jasa. Jika terjadi penyalahgunaan data pribadi oleh perusahaan *e-commerce*, maka pengguna jasa dapat menggugat perusahaan dengan perbuatan melawan hukum, karena pengguna merasa dirugikan dengan adanya penyalahgunaan tersebut.

Kata kunci: Perlindungan Data Pribadi; *E-Commerce*; Privasi.

Abstract

Nowadays, the world is in the beginning of revolution industry 4.0, with one of the example is Big Data. Big Data is an era to collect and maintain every kind of data including personal data. The technology growth changes some of life aspect, such as electronic transaction (e-commerce). In order to enjoy the facility of e-commerce, consumer must input their personal data to the company. Unfortunately, consumer doesn't have any idea how the company keep and maintain their personal data. The lack of understanding leads to big gap of opportunity for misusing the personal data by company or other party. The method used for this research is Normative Juridical, with research specification is with Descriptive Analysis. The type and source of data used in this research is secondary data, collected by literature study from primary, secondary, and tertiary legal materials. The collected data were analyzed by qualitative analysis method. The result of this research could be concluded that personal data is a personal right that should be protected, and this matter is being mention in Constitution of Indonesia. E-Commerce company has an obligation to keep and maintain the consumer's personal data and be aware of personal rights. If the e-commerce company cause any personal data disadvantages, consumer have an opportunity to sue the company for their loss.

Keywords: Personal Data Protection; *E-Commerce*; Privacy.

I. PENDAHULUAN

Teknologi sekarang ini telah berkembang dengan pesat, dan perkembangan ini didukung dengan adanya inovasi dibidang teknologi, dan kita telah memasuki era revolusi industri 4.0, era dimana adanya perpaduan teknologi pada bidang fisik, digital, maupun biologis. Dengan perkembangan teknologi, memacu berbagai pihak untuk melakukan pengumpulan data, dan bersaing untuk memperbesar kapasitas data. Hal ini memunculkan masa baru yang disebut *Big Data*. *Big Data* mengacu pada pengumpulan data dan kemampuan untuk menggunakannya, serta mendapatkan berbagai keuntungan.

Data dapat berupa berbagai macam, salah satunya adalah data pribadi. Data pribadi merupakan salah satu hak asasi manusia (HAM) yang melekat pada individu sejak lahir, dan pada Undang-undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) menyatakan bahwa:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

Dengan demikian, data pribadi menjadi suatu privasi bagi seseorang untuk tidak diganggu kehidupannya.

Dengan memasuki era revolusi industri 4.0, masyarakat menikmati perkembangan teknologi, seperti internet. Dengan menggunakan internet, terjadi banyak perubahan

pada faktor-faktor kehidupan masyarakat, salah satunya pada bidang perekonomian.

Secara umum, transaksi jual beli adalah ketika pembeli dan penjual melakukan transaksi, dan pembeli membayar sejumlah uang kepada penjual atas barang yang dibeli. Dengan perkembangan teknologi, transaksi jual beli memperluas jangkauan sarannya dengan transaksi secara online di internet, atau yang lebih dikenal dengan *electronic commerce (e-commerce)*.

Pada pelaksanaan *e-commerce*, pembeli diminta untuk memasukkan data pribadi pada laman website tersebut, guna keperluan transaksi jual beli. Data yang diinput akan dikelola oleh perusahaan *e-commerce* dan disimpan sebagai *database* milik perusahaan, Dengan memberikan data pribadi kepada perusahaan, berarti pembeli memberikan akses dan menyetujui perusahaan untuk mengakses dan menyimpan data milik pengguna, dan pembeli secara langsung memperoleh hak untuk mendapat perlindungan kerahasiaan data pribadi.

Namun tidak dapat dihindari, bahwa pembeli yang tidak mengetahui cara pengelolaan dan penyimpanan data pribadi mereka di perusahaan *e-commerce*. Ketidaktahuan ini menyebabkan kerentanan atas perlindungan data dan menimbulkan potensi terhadap penyalahgunaan data pribadi, baik oleh perusahaan maupun oleh pihak ketiga.

Penyalahgunaan data pribadi merugikan pemilik data (*data subject*), dan menyebabkan hak

privasi setiap individu dilanggar oleh perusahaan atau pihak ketiga.

Indonesia merupakan negara berkembang dengan pengguna teknologi yang semakin meningkat, namun perkembangan tersebut tidak diiringi dengan penegakkan hukum yang terbaru. Padahal urgensi dalam penyelesaian masalah hukum tentang perlindungan data pribadi sangat dibutuhkan di Indonesia.

Jika dibandingkan negara lain, Indonesia dapat dikatakan tertinggal jauh dalam pelaksanaan perlindungan data pribadi, terlebih pada lingkup ASEAN. Malaysia merupakan negara pertama di ASEAN yang menerapkan peraturan perlindungan data pribadi, dan Singapura dengan pengaturan *Do Not Call Registry* yang khusus untuk warga negara Singapura. Sedangkan selain dari ASEAN, terdapat peraturan perlindungan data pribadi milik Uni Eropa yaitu *General Data Protection Regulation* (GDPR), dan peraturan ini mendorong banyak negara untuk menciptakan peraturan yang serupa untuk diterapkan pada negara masing-masing.

II. METODE

Penelitian hukum ini menggunakan metode penelitian pendekatan hukum yuridis normatif, yaitu pendekatan yang dilakukan dengan meneliti bahan pustaka, dan mengacu pada kaidah hukum yang ada dan melihat kenyataan yang terjadi.¹

Spesifikasi penelitian yang digunakan dalam penelitian ini

berupa penelitian deskriptif analitis. Metode deskriptif adalah prosedur pemecahan masalah dengan menggambarkan keadaan objek penelitian berdasarkan fakta yang ada, selanjutnya dilakukan analisis melalui peraturan-peraturan yang berlaku dikaitkan dengan teori—teori hukum, pendapat para sarjana, praktisi, dan praktek pelaksanaan hukum yang mengangkut latar belakang mengenai perlindungan data pribadi dalam perdagangan elektronik. Analisa penelitian ini diharapkan dapat mengetahui keadaan yang ada pada teori dan praktek, sehingga diharapkan pada akhirnya kegiatan dapat memecahkan masalah yang ada.

Jenis dan sumber data diperoleh melalui *library research* dan *web research*. Data yang dipakai dalam penelitian ini ialah data sekunder yaitu data yang diperoleh seorang peneliti secara tidak langsung dari sumbernya (objek penelitian), tetapi melalui sumber lain. Untuk penelitian hukum normatif, sumber data dapat dibagi menjadi tiga macam, yaitu:²

a. Bahan Hukum Primer

Yaitu bahan hukum yang memiliki sifat mengikat secara yuridis, antara lain.

Ketentuan Peraturan Nasional Indonesia:

1. Undang-Undang Dasar Negara Republik Indonesia 1945;
2. Kitab Undang-undang Hukum Perdata
3. Kitab Undang-undang Hukum Pidana

¹ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. (Jakarta: PT Raja Grafindo Persada, 2004), hlm. 13.

² Suteki dan Galang Taufani, *Metodologi Penelitian Hukum (Filsafat, Teori dan Praktik)*, (Depok : PT. Raja Grafindo Persada, 2018), hlm. 215-216

4. Undang-undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen;
5. Undang-undang Republik Indonesia Nomor 33 Tahun 1999 tentang Hak Asasi Manusia;
6. Undang-undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi;
7. Undang-undang Republik Indonesia Nomor 29 Tahun 2004 tentang Praktik Kedokteran;
8. Undang-undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;
9. Undang-undang Republik Indonesia Nomor 36 Tahun 2009 tentang Kesehatan;
10. Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Ketentuan Peraturan Nasional Malaysia:

1. *Laws of Malaysia Act 658 Electronic Commerce Act 2006*
2. *Laws of Malaysia Act 709 Personal Data Protection Act 2010*

Ketentuan Peraturan Nasional Singapura:

1. *Electronic Transactions Act 2010 (Cap.88)*
2. *Personal Data Protection Act 2012 (No. 26 of 2012)*
- 3.

Ketentuan Peraturan Nasional Uni Eropa:

1. *The General Data Protection Regulation (EU) 2016/679 (GDPR)*

Ketentuan Peraturan Internasional:

1. *Universal Declaration of Human Rights*

b. Bahan Hukum Sekunder

Yaitu bahan-bahan yang erat kaitannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer.³

c. Bahan Hukum Tersier

Yaitu bahan hukum yang memberikan petunjuk, maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder

III. HASIL DAN PEMBAHASAN

A. Perlindungan Hukum atas Data Pribadi sebagai Hak Seseorang dalam Perdagangan Elektronik (*E-Commerce*) di Indonesia

Perlindungan Data Pribadi di Indonesia terbagi menjadi setidaknya 30 undang-undang di Indonesia, yang terbagi menjadi kewenangan pada berbagai bidang, seperti telekomunikasi, kesehatan, kependudukan, keamanan, perekonomian dan sebagainya. Dengan terbaginya menjadi beberapa undang-undang, menimbulkan multitafsir terhadap implementasi perlindungan data pribadi.

Indonesia merupakan negara di Asia Tenggara dengan transaksi e-

³*Ibid*, hlm.216

commerce terbesar dan diperkirakan akan berada diperingkat teratas untuk beberapa tahun kedepan.

Dengan pertumbuhan pengguna *e-commerce* yang pesat, bahaya dalam melakukan transaksi *e-commerce* timbul dan mengancam pembeli atas data pribadi mereka masing-masing.

Kemudahan yang ditawarkan perusahaan *e-commerce* mampu mempertahankan ketertarikan pembeli, walaupun banyak bahaya yang mengancam. Dalam penelitian Syafudin dan Muhammad (2013), terdapat hasil yang berbanding lurus antara tingkat privasi, keamanan dan kepercayaan yang berdampak pada keputusan untuk membeli melalui *e-commerce*.

Pada pelaksanaan, pembeli memasukkan data pribadi kepada perusahaan *e-commerce* dengan harapan bahwa barang yang dibeli dapat segera dikirimkan. Namun pengelolaan dan penyimpanan data pribadi tersebut tidak diketahui oleh pemilik data, padahal data pribadi merupakan hak yang melekat pada diri manusia sejak lahir (hak asasi manusia).

Masyarakat Indonesia sebagai pengguna jasa *e-commerce* memiliki hak pribadi sebagai pemilik data (*data subject*), dimana seseorang memiliki hak untuk memilih dan menentukan dalam memberikan akses kepada pihak ketiga atau tidak. Lalu, menentukan jika data pribadi akan disimpan atau ingin dihapuskan. Pada era digital, masyarakat memiliki kerawanan atas penyalahgunaan data pribadi. Kerawanan ini timbul karena kurangnya perlindungan hukum atas data pribadi, dan timbul kesengajaan

dari pelaku bisnis atau pihak lain untuk mengambil data pribadi milik orang lain.

Sampai dengan hari ini, Indonesia belum memiliki Undang-undang tentang Perlindungan Data Pribadi. Rancangan undang-undang tentang perlindungan data pribadi telah sampai pada tahap pembahasan, dan diharapkan agar dapat selesai sesegera mungkin. Untuk melakukan antisipasi, Kementerian Komunikasi dan Informatika mengeluarkan Peraturan Menteri Komunikasi dan Informatika (Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Sistem Elektronik). Dalam permen tersebut, jika perusahaan gagal untuk melindungi data pribadi konsumen maka perusahaan tersebut dapat dikenakan berbagai sanksi, salah satunya adalah sanksi administrasi.

Jika dibandingkan dengan Malaysia, sebagai negara pertama di ASEAN yang memiliki peraturan perlindungan data pribadi sejak tahun 2013. *Personal Data Protection Act 2010* (PDPA 2010) untuk peraturan perlindungan data pribadi dan *Electronic Commerce Act 2006* untuk peraturan *e-commerce* disektor privat. Pada pelaksanaan pengawasan perlindungan data pribadi, Malaysia memiliki lembaga yang bertugas untuk mengawasi yang bernama Personal Data Protection Commissioner (PDP Commissioner).

Tujuan dari PDPA 2010 adalah menjaga kepentingan data pribadi pemilik data, dan hal ini diharapkan agar masyarakat dapat menentukan sendiri nasib dari data pribadinya. Data dalam PDPA 2010 dibagi menjadi dua, yaitu data secara umum

dan data sensitif. Data secara umum seperti nama, alamat, nomor induk kependudukan, dan sebagainya. Sedangkan data sensitif adalah data yang menyangkut kesehatan fisik, kesehatan mental, maupun pilihan politik, agama atau kepercayaan yang dianut. Segala data yang bersifat sensitive hanya dapat diproses ketika perusahaan telah memperoleh persetujuan dari pemilik data. (*general principle section 6 PDPA 2010*). Pemberitahuan atas penggunaan data pribadi harus diberikan kepada pemilik data dalam bentuk tertulis dan dalam bahasa nasional maupun bahasa Inggris (*disclosure principle*). Ketika data pribadi sudah tidak lagi dibutuhkan oleh perusahaan, maka wajib bagi perusahaan untuk menghapus dan menghilangkan data pemilik data secara permanen. (*retention principle*).

Perusahaan *e-commerce* harus mengikuti tujuh prinsip yang ada di PDPA 2010. Ketika perusahaan tidak mengikuti prinsip tersebut, maka perusahaan akan dikenakan denda sebesar MYR 300.000 ringgit atau/dan dipenjara maksimal 2 (*dua*) tahun, sehingga prinsip PDPA harus dijunjung tinggi.

Singapura sebagai salah satu negara yang maju di ASEAN sudah memiliki peraturan tentang perlindungan data pribadi, yaitu *Personal Data Protection Act 2012* (PDPA). Peraturan tentang *Do Not Call Registry* telah *entry into force* pada tanggal 2 Januari 2014, dan PDPA secara umum mengenai pengumpulan, penggunaan dan pengungkapan data pribadi *entry into force* pada tanggal 2 Juli 2014.

Tujuan dari PDPA adalah mengumpulkan, menggunakan dan mengungkapkan data pribadi oleh organisasi dengan memperhatikan kepentingan individu untuk melindungi data pribadi sendiri dan kebutuhan organisasi untuk mengumpulkan, menggunakan dan mengungkapkan data pribadi dengan alasan yang masuk akal dan layak diterima. PDPA mengenal dua katas individu (*Natural Person*) dan kebutuhan organisasi, dan fokus dari PDPA adalah sektor privat di Singapura.

Data yang digunakan berdasarkan PDPA harus memperoleh persetujuan pemilik data, dan cara pemberian data diperoleh secara tegas diberikan (*expressly given*) atau dianggap telah diberikan (*deemed to be given*). Pemilik data harus mengetahui tujuan dari penggunaan data tersebut, dan data yang diambil harus ada sesuai dengan persetujuan.

Singapura memiliki pengawas nasional khusus untuk perlindungan data pribadi berdasarkan PDPA *section 6*, yaitu *the Personal Data Protection Commission* (PDPC). PDPC mengeluarkan pedoman khusus untuk data pribadi anak dibawah 13 tahun, bahwa orang tua yang memberikan persetujuan atas nama anak tersebut. Pedoman ini dikeluarkan agar penggunaan data pribadi tidak menimbulkan konsekuensi terhadap anak.

PDPA memiliki peraturan yang khusus, yaitu *Do Not Call Registry* (DNC *Registry*). *DNC Registry* menyediakan registrasi bagi warga negara Singapura atau orang yang memiliki nomor telepon Singapura untuk memilih jalan keluar dari

panggilan telepon, pesan teks, dan/atau faksimil. Ada tiga macam DNC Registry, yaitu *No Voice Call Register*, *No Text Message Register*, dan *No Fax Message Register*. DNC Registry dapat dibatalkan jika pemilik nomor telepon meminta untuk dihapuskan.

PDPA tidak menyebutkan pengertian dari *data breach*, namun PDPC mengeluarkan panduan dalam mengelola *data breaches*. Tindakan preventif dari *data breaches* menjadi tanggungjawab *organization* (individu, perusahaan, asosiasi, dan/atau korporasi) yang memiliki tugas untuk melindungi data pribadi dari segala tindakan yang tidak sah dimata hukum.

Sedangkan untuk pelaksanaan *e-commerce* di Singapura, diatur dalam *Electronic Transactions Act* (ETA). ETA mengatur secara spesifik tentang *e-commerce*, *electronic records*, *electronic signatures*, dan sebagainya.

Selain Malaysia dan Singapura, Uni Eropa sebagai negara pelopor untuk mulai membuat peraturan tentang perlindungan data pribadi. *Entry into force* pada 25 Mei 2018 sebagai pengganti dari *the Data Protection Directive*. Peraturan tentang perlindungan data pribadi di Uni Eropa disebut *General Data Protection Regulation* (GDPR).

Tujuan GDPR adalah mengharmonisasikan hukum mengenai privasi data di seluruh Eropa, melindungi dan mendukung semua privasi data milik warga Uni Eropa, dan membentuk kembali cara

organisasi diseluruh regional dalam menghadapi privasi data.⁴

Subjek yang dilindungi dalam GDPR adalah *natural person* atau orang. GDPR berlaku bagi semua pihak yang ada di Uni Eropa, maupun semua pihak yang berada diluar Uni Eropa yang menawarkan barang dan jasa, atau memonitor subjek data milik warga negara Uni Eropa.

Hak yang diatur dalam GDPR adalah hak untuk dilupakan (*right to be forgotten*), dimana setiap subjek data memiliki hak untuk meminta pihak perusahaan *e-commerce* untuk menghapuskan data pribadi mereka tanpa adanya penundaan.

Perlindungan data pribadi bagi anak dibawah umur 16 tahun, proses atas data pribadi akan dianggap sah ketika persetujuan diberikan oleh orang tua anak.

Dalam pengelolaan data pribadi, terdapat dua macam data yaitu data pribadi yang bersifat umum dan data pribadi dengan kategori spesial (*special categories of personal data*). Data pribadi secara umum harus dapat dimanfaatkan untuk mengidentifikasi orang tersebut, yaitu nama, alamat, maupun nomor telepon. Data pribadi dengan kategori spesial adalah data yang menunjukkan ras dan etnis, pilihan politik, agama atau kepercayaan yang dianut.

Jika pada pelaksanaan terjadi kebocoran data, perusahaan *e-commerce* memiliki kewajiban untuk memberitahu kepada *supervisory authority* dalam kurun waktu 72 jam

⁴ Ana Sofa Yuki, Urgensi Peraturan Perlindungan Data Pribadi dalam Era Bisnis *Fintech*. Jurnal Hukum & Pasar Modal Vol. III. ED. 16/2018, hlm. 7.

sejak ditemukannya kebocoran data. Penemuan kebocoran data tersebut harus disertai dengan alasan yang masuk akal.

Kejadian kebocoran data menyebabkan resiko terhadap hak dan kewajiban subjek data, dan informasi kebocoran data harus dikabarkan kepada pemilik data tanpa adanya penundaan. Informasi yang diterima atas kebocoran data harus menggunakan bahasa yang dapat dimengerti oleh pemilik data.

Pengguna jasa harus memahami dan menyetujui terkait penggunaan dan pengelolaan data mereka, termasuk informasi data yang dicari (*cookies*) dan akan diproses oleh perusahaan *e-commerce* untuk dikelola.

Perusahaan *e-commerce* yang tunduk kepada GDPR memiliki kewajiban untuk memiliki *data protection officer* (DPO), yang memiliki fokus untuk memantau strategi dan implementasi perlindungan data pribadi yang diolah pada perusahaan. DPO memiliki tugas untuk mempersiapkan rencana dan strategi jika terjadi kebocoran data kedepannya.

B. Penyalahgunaan Data Pribadi dalam Perdagangan Elektronik dalam Perbuatan yang bersifat Melawan Hukum

Jika terjadi penyalahgunaan atas data pribadi yang disebabkan karena kelalaian perusahaan *e-commerce*, maka perusahaan tersebut dapat dikatakan melakukan perbuatan melawan hukum. Perbuatan untuk melindungi data pribadi konsumen telah diatur dalam

undang-undang. Dengan demikian, perusahaan memiliki kewajiban untuk menepati peraturan yang ada. Perbuatan melawan hukum diatur dalam pasal 1365 KUHPerdara.

Pasal 1365 KUHPerdara mengandung lima unsur, yaitu unsur perbuatan yang melanggar hukum, menimbulkan kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya dan menggantikan kerugian. Perbuatan yang melanggar hukum berarti tindakan yang melanggar hukum secara tertulis dan tidak tertulis.

Kerugian yang dirasakan oleh orang lain dapat berupa kesengajaan maupun kealpaan. Kesalahan terjadi karena saat melakukan perbuatan, sudah memahami konsekuensi yang akan terjadi.

Tindakan yang dilakukan harus memiliki hubungan sebab akibat antara kerugian maupun perbuatan yang dilakukan. Perlindungan yang dilakukan perusahaan dirasa kurang maksimal terhadap data pribadi konsumen dan memiliki hubungan dengan kerugian yang dirasakan oleh konsumennya.

Unsur terakhir adalah kerugian yang dirasakan dapat berupa materiil maupun immateriil. Kerugian yang ditanggung harus kerugian akibat perbuatan perusahaan *e-commerce*.

Jika pemilik data merasakan kerugian atas kebocoran data yang dialaminya, pemilik data dapat mengajukan gugatan perbuatan melawan hukum pada perusahaan *e-commerce*. Kebocoran data pribadi yang terjadi dibawah pengawasan perusahaan tersebut, merupakan tanggungjawab perusahaan yang seharusnya menjaga data tersebut.

Berbeda halnya jika perusahaan *e-commerce* berada di luar Indonesia, maka yurisdiksi wilayah untuk mengadili harus ditentukan oleh kedua belah pihak. Indonesia dapat menerapkan perluasan yurisdiksi teritorial, dimana Indonesia dan negara yang bersangkutan harus memiliki perjanjian ekstradisi, dan tindakan yang dilakukan harus bersifat *double criminality*.

Jika dalam proses pemeriksaan ditemukan adanya delik pidana yang dilakukan oleh perusahaan *e-commerce*, maka perusahaan dapat dikenakan delik pidana berdasarkan UU ITE. Jika perusahaan dianggap menyalahgunakan data pribadi dan menggunakan data tersebut untuk keuntungan pribadi. Perbuatan pidana dalam UU ITE diatur dari pasal 27 sampai pasal 35 UU ITE.

IV. KESIMPULAN

1. Data Pribadi merupakan hak asasi manusia yang harus dilindungi, dapat dilihat pada pasal 28 huruf G UUD 1945. Namun, perlindungan data pribadi di Indonesia sampai saat ini masih sangat lemah, dan hal ini dibuktikan dengan peraturan terkait perlindungan data pribadi masih terbagi menjadi kurang lebih 30 undang-undang.
2. Perusahaan *e-commerce* yang gagal untuk melindungi data pribadi konsumen, dianggap melanggar pasal 1365 KUHP data tentang Perbuatan Melawan Hukum. Selama perusahaan *e-commerce* menyebabkan kerugian bagi konsumen karena suatu perbuatan yang melawan hukum,

maka dianggap sebagai perbuatan melawan hukum. Jika perbuatan perusahaan *e-commerce* mengandung delik pidana, dapat menggunakan dasar hukum UU ITE.

V. DAFTAR PUSTAKA

A. Buku:

- Abdul Kadir Muhammad. *Hukum Perikatan*. Bandung: Citra Aditya Bakti
- Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayatara (Cyber Crime)*. Bandung: Refika Aditama
- Andrea De Mauro, et.al, 2015. *What is Big Data? A Consensual Definition and A Review of Key Research Topics*, AIP Conference Proceedings
- Arsyad M. Sanusi, 2001. *E-Commerce, Hukum dan Solusinya*. Jakarta: PT Mizan Grafika Sarana
- David Konsiur, 1997. *Understanding Electronic Commerce*. Washington: Microsof Press
- Eddy O.S. Hiariej, 2017. *Prinsip-prinsip Hukum Pidana*. Jogjakarta: Cahaya Atma Pustaka
- Farah Mohd Shahwahid dan Surianom Muskam, 2014. *Personal Data Protection Act 2010: Taking the First Steps Toward Compliance*
- Ignatius Ricky Jonathan dan M. Rachman Mulyandi, 2019. *Pengaruh Privasi, Keamanan dan Kepercayaan terhadap Keputusan Pembelian Masyarakat dalam E-*

- Commerce. Prosiding Seminar dan Lokakarya Kualitatif Indonesia*
- J. Satrio, 2001. *Hukum Perikatan, Perikatan yang Lahir dari Undang-undang*. Bandung: Citra Aditya Bakti
- M. A. Moegni, 1982. *Perbuatan Melawan Hukum Cet. 2*. Jakarta: Pradnya Paramita
- Mariam Darus Badruzaman, 2006. *Kitab Undang-Undang Hukum Perdata Buku III tentang Hukum Perikatan dengan Penjelasan*. Bandung: PT Alumni
- Mestika Zed, 2003. *Metode Penelitian Kepustakaan*, Jakarta: Yayasan Obor Indonesia
- Munir Fuady, 1999. *Hukum Kontrak (dari Sudut Pandang Hukum Bisnis)*. Bandung: Citra Aditya Bakti
- Munir Fuady, 2002. *Perbuatan Melawan Hukum (Pendekatan Kontemporer)*. Bandung: Citra Aditya Bakti
- Oktiva Anggraini dan Supriyanto, 2019. *Literasi Digital: Suatu Kemewahan bagi UMKM Perikanan di Era Industri 4.0?, Prosiding Seminar dan Lokakarya Kualitatif Indonesia*
- Onno W. Purbo dan Aang Arif Wahyudi, 2001. *Mengenal E-Commerce*. Jakarta: Elex Media Komputindo
- Richard Eko Indrajit, 2001. *E-Commerce: Kiat dan Strategi Bisnis di Dunia Maya*. Jakarta: Elex Media Komputindo
- Roeslan Saleh, 1981. *Sifat Melawan Hukum dari Perbuatan Pidana*. Jakarta: Aksara Baru
- Rosa Agustina, 2003. *Perbuatan Melawan Hukum Cet. 1*. Jakarta: Program Pascasarjana FH UI
- Vollmar, 1984. *Pengantar Studi Hukum Perdata*. Jakarta: CV Rajawali
- Warren B. Chik, 2014. *The Singapore Do Not Call Register and the Text and Fax Exemption Order*. Research Collection School of Law.
- B. Jurnal:**
- Ana Sofa Yuking, 2018. *Urgensi Peraturan Perlindungan Data Pribadi dalam Era Bisnis Fintech*, Jurnal Hukum & Pasar Modal Volume III
- Lembaga Studi & Advokasi Masyarakat, 2017. *Membersarnya Potensi Ancaman Terhadap Kebebasan Sipil dan Memudarnya Peran Negara dalam Perlindungan HAM*
- Lia Sautunnida, 2018. *Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia*. Kanun Jurnal Ilmu Hukum Volume 20 Nomor 2
- Rosalinda Elsina Latumahina, 2014. *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal Gema Aktualita Volume 3 Nomor 3.



- Samuel D. Warren dan Louis D. Brandeis, 1890. *The Right to Privacy*. Harvard Law Review Volume IV.
- Sinta Dewi, 2016. *Konsep Perlindungan Hukum atas Privasi dan Data Pribadi dikaitkan dengan Penggunaan Cloud Computing di Indonesia*. Yustisia Volume 5 Nomor 1.
- Sinta Dewi Rosadi, 2018. *Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia*. Brawijaya Law Journal Volume 5 Nomor 1
- William Posser, 1984. *Privacy: A Legal Analysis*. Cambridge University Press