KERIS Jurnal DEFENDONESIA
ISSN: 2354-6964

Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia

Meha Middlyne Simbolon[1], I Gusti Komang Wijaya Kesuma[2].
Aditya Ery Wibowo[3].

Abstrak

E-commerce sebagai aktifitas perdagangan melalui jaringan elektronik, merubah jenis transaksi konvensional menjadi transaksi pasar maya. *E-Commerce* tentunya memberikan pengaruh yang masif terhadap perkembangan ekonomi digital. *In casu a quo*, perkembangan teknologi digital semakin erat kaitannya dengan timbulnya kejahatan siber yang mengancam pertahanan dan keamanan negara yang berpotensi menghambat laju pertumbuhan ekonomi. Sistem transaksi *e-commerce* yang digunakan oleh pengguna harus menanggung banyak risiko ditambah dengan perilaku *cyber crime* masih sangat sulit di antasipasi oleh pengguna dan penyedia. Oleh karena itu, perdagangan berbasis sistem elektronik harus dilindungi keamanannya oleh pemerintah dengan melakukan koordinasi yang bersifat lini sektoral, perluasan kewenangan, dan membentuk beberapa kebijakan baru dalam pengamanan dan penindakan terhadap *e-commerce*.

Kata Kunci: Perdagangan Berbasis Sistem Elektronik, Kejahatan Siber, Pertumbuhan Ekonomi Digital.

[1] Penulis merupakan mahasiswa aktif Fakultas Hukum di Universitas Gadjah Mada, Yogyakarta. Angkatan 2017, mehamiddlynesimbolon@gmail.com.
[2] Penulis merupakan mahasiswa aktif Fakultas Hukum di Universitas Gadjah Mada, Yogyakarta. Angkatan 2019, dan aktif dalam kepengurusan di Satria Paramartha. Komangwijayagusti@gmail.com
[3] Penulis merupakan mahasiswa aktif Fakultas Hukum di Universitas Gadjah Mada, Yogyakarta. Angkatan 2019, dan aktif dalam kepengurusan di Dewan Mahasiswa Fakultas Hukum Universitas Gadjah Mada. Adityaeri22@gmail.com

KERIS Lembaga Kajian Pertahanan Strategis
Jurnal DEFENDONESIA
ISSN: 2354-6964

PENDAHULUAN

Proses transaksi yang dilakukan dalam dunia bisnis, tanpa adanya pertemuan antar pihak dengan menggunakan media internet dikategorikan sebagai transaksi elektronik. Transaksi elektronik dalam dunia bisnis terdapat berbagai macam bentuk, salah satunya adalah *electronic commerce (e-commerce*) atau secara gramatikal diartikan sebagai perdagangan yang dilakukan secara elektronik, berhubungan dengan kegiatan transaksi komersial dengan menggunakan internet sebagai media untuk menyediakan layanan *get and delivery*. Aktivitas perdagangan sangat dirasakan manfaatnya, karena sifatnya yang *borderless*, sehingga dapat menekan biaya operasional, mempercepat waktu pemrosesan dan mengurangi risiko terjadinya *human error.*[4]

Sistem keamanan pada *e-commerce* yang digunakan adalah jenis *secure socket layer* (SSL)[5] sedangkan sistem pengesahan pembayaran kartu kredit menggunakan bantuan pihak ketiga yang dipercaya oleh penyelenggara jasa kartu kredit dan institusi keuangan yang digunakan pengelola, yang disebut sebagai pemroses pembayaran (*payment processor/ payment gateway*).[6]

Namun, seiring dengan penerapan teknologi di setiap dimensi kehidupan manusia, ternyata diikuti pula dengan penyalahgunaan teknologi dalam ranah siber untuk tujuan kejahatan. Munculnya kejahatan siber merupakan suatu pembenaran, bahwa era global ini identik dengan era ranjau ganas. Sebuah ruang imajiner dan maya, area atau zona bagi setiap orang untuk melakukan aktivitas yang bisa dilakukan dalam kehidupan sosial sehari-hari dengan cara artifisial. Paradigma keamanan dan pertahanan

---

4 *Human error* adalah suatu keputusan atau tindakan yang mengurangi atau potensial untuk mengurangi efektivitas, keamanan atau performansi suatu sistem. Lihat Desriyani ilaen. Human Error pada Interaksi Manusia dengan Komputer. *https://medium.com/@desriyanisilaen/human-error-pada-interaksi-manusia-dengan-komputer-beb6d04f543c*. 22 Januari 2021 (09.15).

5 SSL dilengkapi juga dengan teknik pengacakan data (*encryption*) dengan metode *Message Authetification Code* (MAC).

6 Data-data calon pembeli termasuk nomor kartu kredit dan identitas lain, secara langsung terenkripsi oleh *Commercenet*. Lihat Christina Widyasari, 2005, Penggunaan *E-Commerce* Pada Aplikasi Penjualan Adidas (*Usage of At Application Sale of Adidas*), Skripsi, Fakultas Ilmu Terapan Program Studi Teknik Informatika, Hlm. 4.

nasional telah bergeser kepada aspek lebih luas yakni jaminan keamanan pribadi warga negara dan pertumbuhan sekaligus perkembangan perekonomian nasional. Berdasarkan data Pusat Operasi Kemanan Siber Nasional, terdapat 16.503.193 serangan siber pada Mei 2020. Angka tersebut naik tajam dibandingkan dengan Mei 2019, dengan jumlah total serangan mencapai 5.678.713 serangan.[7]

Ancaman keamanan yang lazim terjadi pada *e-commerce* adalah serangan *phising* yang berujung pada kasus pencucian uang, penyalahgunaan data, *hacking*, penipuan kartu kredit dan layanan yang tidak dilindungi. Contohnya, kasus order fiktif Lazada senilai 22 juta rupiah pada tahun 2018, dimana transaksi fiktif dilakukan oleh pembobol dengan cara masuk ke *email* pengguna kemudian membaca kode verifikasi dari kartu kredit pengguna. Berikutnya, yang tidak kalah menarik adalah kasus Tokopedia yang menuai banyak kritik, dimana data 91 juta pengguna Tokopedia diretas dan diperjualbelikan di situs gelap (*dark web*). Tentunya aktivitas perekonomian digital akan semakin terpuruk, apabila tidak diikuti dengan struktur pengamanan yang baik. Struktur pengamanan yang baik tidak hanya dilihat dari fungsi regulasi maupun tataran kebijakan dalam rangka penanganan kejahatan siber, tetapi juga tata kelola kewenangan yang baik, yang melibatkan kolaborasi lini sektoral. Sebagaimana amanat dari Pasal 31 ayat (5) Undang-Undang Negara Republik Indonesia 1945 bahwa Pemerintah memajukan ilmu pengetahuan dan teknologi dengan menjunjung tinggi nilai-nilai agama dan persatuan bangsa untuk kemajuan peradaban serta kesejahteraan umat manusia.[8]

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian normatif, dengan menggunakan beberapa pendekatan penelitian hukum (*legal research*)[9] antara lain, pendekatan peraturan perundang-undangan (*statute approach*) dilakukan dengan menelaah semua peraturan perundang-undangan terkait. [10] Lalu pendekatan konseptual (*conceptual approach*) dilakukan dengan mempelajari pandangan-pandangan di dalam ilmu hukum. [11] Metode penelitian yang digunakan dalam karya tulis ini

[7] Tim Kompas. Jumlah Serangan Siber Meningkat. *https://www.cissrec.org/news/detail/730/Jumlah-Serangan-Siber-Meningkat.html*. 30 Januari 2021 (08.03).

[8] Lihat Pasal 31 ayat (5) Undang-Undang Negara Republik Indonesia 1945.

[9] Johnny Ibrahim. 2006. *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing. Malang. Hlm. 30.

[10] Peter Mahmud Marzuki. 2005. *Penelitian Hukum*. Kencana. Jakarta. Hlm. 94.

[11] *Op. Cit.* Hlm. 95.

adalah metode kualitatif non-intreraktif. Metode kualitatif menitikberatkan pada analisis logis serta deskripsi dan penyimpulan naratif atau kata-kata.[12]

Kesiapan Instrumen Penyelenggaraan Perdagangan Melalui Sistem Elektronik Serta Pengaruhnya Terhadap Timbulnya Kejahatan Siber

1. Legalitas *Terms and Conditions* Pengoperasian Perdagangan Melalui Sistem Elektronik

Terms and conditions yang disediakan antar penyedia layanan berbeda dikarenakan belum mengadopsi regulasi yang ada di Indonesia. Pertama, mengenai perolehan dan pengumpulan data pengguna. Permintaan data dan informasi pengguna ditujukan untuk mendaftarkan nama, *username*, *email*, alamat, nomor telefon, dan lainnya. Secara otomatis, penyedia juga turut merekam data-data lain seperti data lokasi *riil*, data perangkat, hingga *log* pengguna. [13] Kedua, mengenai penggunaan data. Perolehan dan pengumpulan data ditujukan untuk kepentingan akses dan komunikasi interaktif seperti pemanfaatan fitur pesan, ulasan, diskusi produk, dan sebagainya.

Dalam penyelenggaraannya, *e-commerce* juga melibatkan jasa logistik dalam pengiriman barang/ jasa yang harus diperhatikan. Kejahatan bisa timbul dikarenakan adanya pengalihan data dari penyelenggara dengan pihak jasa logistik. Disisi lain, penyelenggaraan sistem elektronik baik dalam hal proteksi keamanan maupun standarisasi manajemen, tidak menutup kemungkinan bekerja sama dengan pihak ketiga. Pihak ketiga difungsikan untuk memastikan bahwa sistem berjalan dengan baik, sehingga *platform* tersebut dapat terhindar dari serangan-serangan siber yang mengakibatkan malfungsi.[14]

Tersedianya persyaratan *online* akan mengurangi beberapa argumen bahwa konsumen dapat memahami tentang kecurangan, kemustahilan atau ketidakwajaran. Perlindungan data pribadi merupakan hal yang penting bagi konsumen itu sendiri dalam melakukan transaksi *online*. Sebab, data pribadi tersebut berhubungan dengan kemanan konsumen itu sendiri. Sesuai dengan ketentuan Pasal 4 Rancangan Undang-

[12] Asep Saepul Hamdi. 2014. *Metode Penelitian Kuantitatif Aplikasi dalam Pendidikan*. Deepublish. Yogyakarta. Hlm. 4.

[13] Hasil tinjauan terhadap *Terms and Conditions* Kebijakan Privasi di Tokopedia, Shopee, Bukalapak, Lazada, dan OLX.

[14] Hasil wawancara dengan Bapak Ferry Indrawan, S.H., selaku Kepala Bagian Hukum dan Kerjasama Biro Hukum dan Hubungan Masyarakat Sekretariat Utama Badan Siber dan Sandi Negara melalui *zoom meeting* pada 5 Februari 2021.

Undang Perlindungan Data Pribadi (RUU PDP), yang menyebutkan bahwa pemilik data pribadi berhak meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data pribadi.[15]

Sangat disayangkan, prinsip utama transaksi secara *online* di Indonesia masih lebih mengedepankan aspek kepercayaan (*trust*) terhadap penjual maupun pembeli. Artinya aturan-aturan teknis terkait *code of conduct* dari akivitas tersebut diharapkan mampu melindungi kepentingan konsumen melalui *privacy policy* yang berlaku dalam setiap kegiatan agar disepakati kedua belah pihak.

2. Bentuk Koordinasi Antara Kementerian/ Lembaga/ Instansi (K/L/I) yang Menangani *Internet of things* dan dunia digital sebagai sarana interaksi dan transaksi, membuat kegiatan perekonomian pun ikut berubah. Aktivitas dunia siber di Indonesia hanya dipayungi oleh 2 (dua) kerangka hukum, yakni Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)[16] dan Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Perkominfo 20/2016).

Ancaman siber yang bersifat multidimensional membutuhkan koordinasi antar Kementerian /Lembaga /Instansi (K/L/I), seperti Kementerian Komunikasi dan Informasi (Kemenkominfo), Badan Siber dan Sandi Negara (BSSN), dan Institusi Tentara Nasional Indonesia (TNI) dan/atau Kepolisian Negara Republik Indonesia (Polri). Sinergi antar lembaga ini ditujukan untuk membangun dan memelihara keamanan siber nasional yang optimal, guna melindungi infrastruktur telekomunikasi dan siber dari situasi kritis yang dikenal dengan *The National Cyber Space Response System.* Permasalahan koordinasi pengamanan siber nasional oleh BSSN dirasa belum maksimal karena masih berada di tahap awal ditambah dengan adanya perbedaan struktur dalam penanganan keamanan siber antar lembaga.

Pengalihan tugas dan tanggungjawab terhadap pengkoordinasian keamanan siber melalui Kominfo kepada BSSN telah ditindaklanjuti dengan penyusunan struktur organisasi pada BSSN dan penyesuaian struktur pada Kominfo.

[15] Pasal 4 Rancangan Undang-Undang Perlindungan Data Pribadi.

[16] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Namun, dalam pelaksanaannya, BSSN masih sepenuhnya bergantung pada regulasi yang ada pada Kominfo. Peran Kominfo sebagai pendukung pelaksanaan keamanan siber dari aspek infrastruktur telekomunikasi dan informatika, masih perlu diperjelas dalam sebuah regulasi yang bersifat operasional. Terbatasnya wewenang BSSN [17] dalam menjaga keamanan dan ketahanan siber nasional, BSSN pada praktiknya hanya mampu untuk me-*monitoring* kegiatan yang ada di dalam ruang siber tanpa bisa melakukan penindakan. Kewenangan penindakan dilaksanakan oleh Kominfo.[18] Pada bulan Juli 2020, BSSN telah membuat suatu kebijakan, yaitu dengan mengadakan Pusat Malware Nasional (PUSMANAS), tetapi lambatnya proses penyusunan regulasi mempengaruhi rancangan program PUSMANAS masih pada tahap ditangguhkan. [19] PUSMANAS akan bergerak pada bidang penyelengaraan *Malware Repository Frame Work* (MRF) dan *Cyber Threat Information Sharing* (CTI) yang diharapkan mampu menampung, mengolah, menganalisis setiap *malware* dan serangan siber, serta tempat untuk berbagi informasi terkait ancaman atau informasi tentang serangan siber dengan pihak terkait.[20]

3. Ketentuan Penyelenggaraan Sistem Elektronik

Perdagangan melalui sistem elektronik termasuk dalam pengertian badan usaha yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik, sebagaimana definisi Penyelenggara Sistem Elektronik pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. [21] Hal ini menandakan bahwa badan atau perusahaan yang melakukan perdagangan melalui sistem elektronik

[17] Pasal 3 Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

[18] Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.
Lihat Pasal 43 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[19] Hasil pemaparan dari Dr. Sulistyo, S. SI, S.T., M.Si selaku Direktur Deteksi Ancaman BSSN Pada Webinar Mengenai "Peningkatan Kualitas Deteksi Ancaman Siber Melalui Pusat Malware Nasional" yang diselenggarakan pada 14 Juli 2021 melalui Kanal YouTube BSSN.

[20] *Ibid.*

[21] Pasal 2 ayat 5 huruf b Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

wajib terdaftar sebagai Penyelenggara Sistem Elektronik (PSE) dan diawasi oleh Kementerian atau Lembaga berdasarkan ketentuan perundang-undangan.

Dalam menjalankan dan mengoperasikan sistem elektronik, setiap PSE harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.[22] Pemberlakuan aturan-aturan tersebut tidak hanya mengikat bagi PSE pada sektor privat dalam negeri, tetapi juga bagi PSE luar wilayah Indonesia yang melakukan usaha atau sistem elektroniknya yang dipergunakan di wilayah hukum Indonesia.[23] Apabila badan usaha perdagangan melalui mekanisme elektronik tidak terdaftar dalam PSE, maka akan dikenakan sanksi teguran tertulis hingga penghentian sementara terhadap badan usaha yang bersangkutan.[24]

Sampai dengan saat ini, satu-satunya pengaturan standar keamanan informasi hanya diatur dalam Perkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, yang tentunya belum mencukupi untuk memberikan standarisasi dalam pengaturan keamanan PSE.[25] Pertama, terkait pembinaan dan pengawasan sumber daya manusia. Pemerintah tidak dapat melakukan pemantauan atau *monitoring* terhadap semua PSE karena jumlahnya yang sangat banyak dan cakupannya yang sangat luas. Oleh karena itu, pendekatan metode pengendalian keamanan siber penyelenggara elektronik seharusnya diterapkan dengan memetakan PSE sesuai dengan standar risiko dan mekanisme setiap penyelenggara untuk melakukan pengawasan dan pengendalian terhadap PSE.[26] Dalam mewujudkan sistem keamanan yang baik dari setiap PSE tidak hanya bertumpu pada pemerintah saja, namun sektor privat memiliki kewajiban yang sama untuk mewujudkannya.[27]

Kedua, mengenai kepatuhan pengamanan PSE masih menjadi

[22] Pasal 3 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[23] Pasal 21 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[24] Pasal 100 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[25] Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi.
[26] Hasil pemaparan dari Teguh Arifyadi, S.H., M.H. selaku Ketua Umum Indonesia Cyber Law Community Pada Webinar Mengenai "Wajib Tau! Tips-Tips Keamanan Siber Langsung Dari Pakarnya" yang diselenggarakan pada 28 Juni 2020 melalui Kanal YouTube Klinik Hukum*online*.
[27] *Ibid.*

permasalahan[28], karena hingga saat ini, sanksi yang diterapkan terhadap pengingkaran kewajiban setiap PSE pun belum jelas, bersifat tidak memaksa, dan tidak memberikan efek jera. Ketiga, penyediaan rekam jejak audit. Salah satu kewajiban PSE adalah menyediakan rekam jejak audit, namun pada faktanya tidak semua penyelenggara mempunyai rekam jejak audit. Keempat, penyelenggara wajib melakukan pengamanan terhadap komponen PSE. Tetapi belum ada sistem pencegahan dan Standar Operasional Prosedur (SOP) untuk melindungi komponen penyelenggara. Berdasarkan kasus-kasus kebocoran data pribadi pengguna, PSE cenderung menutupi kasus tersebut dan menunggu adanya laporan terlebih dahulu dari nasabah karena khawatir adanya krisis kepercayaan konsumen yang akan berdampak pada keuntungan perusahaan. Hal ini menandakan bahwa aturan-aturan yang ada harus diperkuat dan ditegakkan kembali agar pengamanan PSE dapat berjalan dengan baik. Dari uraian di atas dapat disimpulkan bahwa permasalahan utama terdapat pada minimnya penerapan aturan-aturan dan kewajiban-kewajiban yang seharusnya dilaksanakan oleh PSE. Jika peraturan-peraturan yang telah ada dapat dipatuhi oleh PSE, maka akan memberi sebuah nilai positif terkait dengan pengembangan keamanan siber.

Berikutnya, hal yang patut diperhatikan adalah penerapan standar sistem manajemen pengamanan informasi, sebagaimana yang diatur dalam Pasal 7 Perkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang menyatakan bahwa PSE tingkat tinggi harus menerapkan ISO/IEC 27001. Meskipun ISO 27001 merupakan *legal formal* yang bersifat global, tetapi ruang lingkup yang diatur dalam ISO 27001 ini hanya sebatas ruang lingkup manajemen. Artinya, meskipun dilakukan sertifikasi dengan melakukan pengecekan penetrasi, uji coba untuk mengetes adanya suatu celah atau tidak, tetapi hal-hal yang berkaitan dengan teknis ini tidak selalu diperiksa secara berkala. [29] Perusahaan yang telah tersertifikasi *Lead Auditor* ISO 27001 belum tentu mumpuni dalam pelindungan data pribadi dikarenakan kemampuan perusahaan

[28] Salah satu sanksi administratifnya hanya sebatas pengumuman di situs dalam jaringan.
Lihat Pasal 36 Peraturan Menteri Komunikasi Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

[29] Hasil wawancara dengan Baderi, S.Sos., M.E., C.CISO., selaku Kepala Sub Direktorat Proteksi Informasi Perdagangan Berbasis Elektronik BSSN melalui *zoom meeting* pada 2 Februari 2021.

dalam mengamankan informasi harus kembali diaudit setiap tahunnya.[30]

Kemudian keamanan *data center* yang berisi tentang pengklasifikasian data sesuai dengan kategori jenis data yang diamankan masih belum diterapkan pada standar keamanan ISO 27001. Hal-hal demikian yang tidak di atur dalam ruang lingkup manajemen yang menyebabkan kurang maksimalnya penggunaan standar ISO 27001. Selain itu, permasalahan lain yang sangat substansial terkait PSE hingga saat ini, yaitu belum adanya lembaga yang secara khusus menangani dan mengawasi kepatuhan dan pelaksanaan manajemen sistem keamanan PSE. Padahal bagian yang paling terpenting dari eksistensi suatu produk hukum adalah penegakan dan penerapannya. Karena regulasi yang efektif bukan seberapa detail regulasi itu dibuat, tetapi seberapa tangguh regulasi itu ditegakkan.[31]

PENUTUP

Instrumen penyelenggaraan perdagangan berbasis sistem elektronik di Indonesia hingga saat ini belum sepenuhnya siap untuk dapat menyelenggarakan perdagangan berbasis sistem elektronik. Hal ini disebabkan oleh karena belum adanya instrumen yang menjadi acuan dasar, sehingga masih menggunakan instrumen yang parsial dan tersebar pada berbagai macam produk hukum. Pada penyelenggaraannya, Rancangan Undang-Undang Perlindungan Data Pribadi dan Rancangan Undang-Undang Kejahatan dan Keamanan Siber dapat menjadi jawaban untuk mengatur aktivitas penggunaan data pribadi di Indonesia, khususnya dalam aktivitas peralihan data dari pemilik data kepada *e-commerce*, serta sarana pengaturan media tempat aktivitas peralihan data tersebut terjadi untuk memberikan pengamanan (*safeguard*) terhadap perdagangan melalui sistem elektronik sebagai langkah percepatan pertumbuhan ekonomi digital.

[30] *Ibid*..
[31] *Ibid.*

DAFTAR PUSTAKA

A. BUKU

Hamdi, Asep Saepul. 2014. *Metode Penelitian Kuantitatif Aplikasi dalam Pendidikan.* Deepublish. Yogyakarta.

Ibrahim, Johnny. 2006. *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing Malang.

Kristiyanti, Celina Trwi Siwi. 2011. *Hukum Perlindungan Konsumen*. Sinar Grafika. Jakarta.

Marzuki, Peter Mahmud. 2005. *Penelitian Hukum*. Kencana. Jakarta.

Wahid, Abdul dan Labib, Mohammad. 2005. *Kejahatan Mayantara (Cyber Crime)*. PT Refika Aditama. Bandung.

Widodo dan Utami, Wiwik. 2014. *Hukum Pidana dan Penologi: Rekonstruksi Model Pembinaan Berbasis Kompetensi Bagi Terpidana Cybercrime.* Aswaja Pressindo. Yogyakarta.

B. PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. 25 November 2016. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik. 10 Oktober 2019. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. 1 Desember 2016. Berita Negara Republik Indonesia Nomor 1829 Tahun 2016.

Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. 11 April 2016. Berita Negara Republik Indonesia Nomor 551 Tahun 2016.

C. TUGAS AKHIR

Widyasari, Christina. 2005. Penggunaan *E-Commerce* Pada Aplikasi Penjualan Adidas (*Usage of At Application Sale of Adidas*). Skripsi. Fakultas Ilmu Terapan Program Studi Teknik Informatika.

Suseno, Wahyu Hanggoro, 2008, *Kontrak Perdagangan Melalui Internet (Electronic Commerce) Ditinjau dari Hukum Perjanjian*. Skripsi. Program Sarjana Fakultas Hukum Universitas Sebelas Maret. Surakarta.

D. JURNAL DAN ARTIKEL

Ardiyanti, Hardini. Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global: *Indonesia Security Incident Response Team On Internet Infrastructure* (Id-Sirtii). 5(6): 100.

Indriyani, Masitoh. Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada *Online* Market Place System. *Jurnal Justitia Fakulas Hukum Universitas Muhammadiyah Surabaya*. Vol. 1(2): 196.

Kusuma Dewi, Sri Anggaraini. Perjanjian Jual Beli Barang Melalui *Electronic Commerce* (*E-Com*). *Jurnal Ilmiah Teknologi dan Informasi Asia (JITIKA)*, 9(2): 1.

Maulana, Shabur Miftah dan Susilo, Heru. Implementasi *E-Commerce* Sebagai Media Penjualan *Online* (Studi Kasus Pada Toko Pastbrik Kota Malang). *Jurnal Administrasi Bisnis*. 29(1): 2

.

Silalahi, dkk. Sinergitas BSSN dan Kominfo Dalam Meningkatkan Kesiapan Cyber Security Pada Sektor *E-Commerce* Di Indonesia. *Jurnal Peperangan Asimetris*. 5(8): 28.

E. INTERNET

Ilaen, Desriyani. Human Error pada Interaksi Manusia dengan Komputer. *https://medium.com/@desriyanisilaen/human-error-pada-interaksi-manusia-dengan-komputer-beb6d04f543c*. 22 Januari 2021 (09.15).

Burhan, Fahmi Ahmad. Mengapa E-Commerce jadi Sasaan Empuk Pembobolan Data?. *https://katadata.co.id/agustiyanti/digital/5eb2c78109940/mengapa-e-commerce-jadi-sasaran-empuk-pembobolan-data*. 30 Januari 2021 (13.09).

Cahya, Indra. Kasus Order Fiktif Lazada Sebesar 22 Juta, Ini Kronologisnya!. *https://www.merdeka.com/teknologi/kasus-order-fiktif-lazada-sebesar-22-juta-ini-kronologisnya.html*. 30 Januari 2021 (11:18).

Letkol Chb Ir. Bagus Artiadi Soewardy, M.Si. Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh Bagi Indonesia. *https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence*.pdf. 29 Januari 2021 (15.02).

Mediana. Ancaman Serangan Siber Bersifat Multidimensi", *https://kompas.id/baca/ekonomi/2017/06/05/ancaman-serangan-siber-bersifat-multidimensi*. 6 Februari 2021 (16.05).

Wardoyo, Savira. Tokopedia Dibayangi Krisis Kepercayaan Dari Konsumen. *https://www.cnbcindonesia.com/tech/20210505204833-37-156559/tokopedia-dibayangi-krisis-kepercayaan-dari-konsumen*. 6 Februari 2021 (18.22).

Chairil, Tangguh. Mewujudkan Keamanan Siber Bagi Indonesia Apa Yang Harus Dilakukan. *https://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813*. 6 Februari 2021 (20.01).

Gobel, Tenri. BSN Minta Marketplace Terapkan ISO 27001:2013 untuk Keamanan. *https://cyberthreat.id/read/6666/BSN-Minta-Marketplace-Terapkan-ISO-270012013-untuk-Keamanan*. 6 Februari 2021 (20:22).

Kompas, Tim. Jumlah Serangan Siber Meningkat. *https://www.cissrec.org/news/detail/730/Jumlah-Serangan-Siber-Meningkat.html*. 30 Januari 2021 (08.03).

Mahrus, Zuhri. Kebocoran Data Pengguna Tokopedia, Bukalapak, dan Bhinneka: Siapa Peduli?", *https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli*. 25 Januari 2021 (14.00).