Jurnal Kritis Studi Hukum

Vol. 9 No. 4 Tahun 2024
Halaman 74-80

URGENSI PENGGUNAAN SERTIFIKAT KEANDALAN KATEGORI KEAMANAN SISTEM ELEKTRONIK BAGI PELAKU E-COMMERCE DI INDONESIA

Aryani Mustika Permatasari[1], Muhamad Amirulloh[2], Danrivanto Budhijanto[3]
aryani2001@mail.unpad.ac.id[1], muhamad.amirulloh@unpad.ac.id[2], danrivanto@unpad.ac.id[3]
Universitas Padjadjaran

Abstrak

E-commerce yang dilakukan melalui internet selain memberikan keuntungan, juga berpotensi menimbulkan kerugian dikarenakan *vulnerability* dalam sistem elektronik *e-commerce* terhadap berbagai ancaman gangguan atau serangan siber. Sertifikat Keandalan Keamanan Sistem elektronik mengacu pada standar sistem pengamanan yang diatur oleh PBSSN 8/2020 yaitu SNI ISO/IEC 27001. Dalam kepentingan keamanan sistem elektronik, BSSN berwenang menetapkan pemberlakuan SNI wajib berdasarkan UU SPK 20/2014. Dalam menjamin keandalan dan keamanan sistem elektronik PP PMSE 80/2019, PBSSN 8/2020, dan UU SPK 20/2014 mewajibkan kepada pelaku *e-commerce* untuk menggunakan Sertifikat Keandalan Keamanan sistem elektronik SNI ISO/IEC 27001 untuk melindungi konsumen dalam transaksi elektronik. Penelitian ini mempunyai tujuan untuk mengetahui bagaimana pelaksanaan kewajiban penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik oleh pelaku *e-commerce* di Indonesia dan bagaimana tanggung jawab pelaku *e-commerce* terkait penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik. Metode pendekatan yuridis normatif digunakan dalam penelitian ini dengan mengkaji bahan hukum primer yaitu peraturan perundang-undangan serta bahan hukum sekunder yaitu jurnal dan buku. Hasil penelitian ini menunjukkan bahwa belum semua pelaku *e-commerce* mematuhi ketentuan tentang penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001 sebagaimana diwajibkan PP PMSE 80/2019, PBSSN 8/2020, dan UU SPK 20/2014. Pelaku *e-commerce* yang tidak *comply* dengan kewajiban tersebut berpotensi melanggar hukum maka, pelaku *e-commerce* dapat dikenakan sanksi secara administratif, perdata, dan pidana. Pelaku *e-commerce* sebaiknya segera memperoleh sertifikat keandalan keamanan sistem elektronik agar menjamin keandalan dan keamanan sistem elektroniknya.

Kata Kunci: Sertifikat Keandalan, E-commerce, Hukum siber.

ABSTRACT

E-commerce carried out via the internet, apart from providing benefits, also has the potential to cause losses due to the vulnerability of e-commerce electronic systems to various threats of disruption or cyber-attacks. The Electronic System Security Reliability Certificate refers to the security system standard regulated by PBSSN 8/2020, namely SNI ISO/IEC 27001. In the interest of electronic system security, BSSN is authorized to determine the mandatory implementation of SNI based on SPK Law 20/2014. In ensuring the reliability and security of electronic systems, PP PMSE 80/2019, PBSSN 8/2020, and SPK Law 20/2014 have required all e-commerce actors to use the SNI Mandatory ISO/IEC 27001 Electronic System Security Reliability Certificate to protect consumers in electronic transactions. This research attempts to ascertain out how the implementation of the obligation to use the Electronic System Security Reliability Certificate by e-commerce actors in Indonesia and the responsibility of e-commerce actors in the use of the Electronic System Security Reliability Certificate. This research uses a normative juridical approach method by study secondary legal materials in the form of books and journals and primary legal materials in the form of laws and regulations. The results showed that not all e-commerce actors have complied with the provisions regarding the use of the SNI ISO/IEC 27001

Electronic System Security Reliability Certificate as required by PP PMSE 80/2019, PBSSN 8/2020, and SPK Law 20/2014. E-commerce actors who do not comply with these obligations have the potential to violate the law, so e-commerce actors can be subject to criminal, civil, administrative sanctions. E-commerce actors should immediately obtain an electronic system security reliability certificate to ensure the reliability and security of their electronic systems.
Keywords: *Reliability Certificate, E-Commerce, Cyber Law*.

PENDAHULUAN

Perkembangan Teknologi berperan penting mempengaruhi kehidupan manusia, termasuk ekonomi. Berkembangnya transaksi perdagangan menandakan ekonomi digital yang memanfaatkan media digital dalam kegiatan ekonomi tanpa harus bertatap muka dalam proses transaksinya, salah satunya dengan *e-commerce* atau Perdagangan Melalui Sistem Elektronik (PMSE). Berikut beberapa contoh pelaku *e-commerce* di Indonesia diantaranya: Tokopedia, Shopee, Buka Lapak, Blibli.com, dan lainnya. Masyarakat memanfaatkan teknologi *e-commerce* untuk memenuhi kebutuhan hidupnya dengan melakukan kegiatannya dengan melalui sistem elektronik atau disebut *cyber space* atau ruang siber (Budhijanto, 2021), membutuhkan pendekatan hukum dan teknologi. Hukum siber adalah aspek hukum dengan lingkup aspek-aspek yang terkait dengan subyek hukum berhubungan dengan TIK melalui internet, termasuk melalui *e-commerce*.(Ramli, 2019). *E-commerce* merupakan perdagangan yang melakukan transaksi nya dengan serangkaian prosedur atau perangkat elektronik.

E-commerce selain memberikan keuntungan dengan dilakukan melalui internet, juga berpotensi menimbulkan kerugian dikarenakan *vulnerability* dalam sistem elektronik *e-commerce* terhadap berbagai ancaman gangguan atau serangan siber *(cyber-attack*) (Patel, 2021). Apabila *e-commerce* terganggu, maka akan berpengaruh terhadap ekonomi yang merupakan roda penggerak utama suatu negara, khususnya ekonomi digital. Dalam hukum siber diatur mengenai pelindungan hukum *e-commerce* tercantum pada UU ITE. Untuk menghindari gangguan-gangguan pada sistem elektronik *e-commerce*, keandalan dan keamanan *e-commerce* harus terjamin supaya keberlangsung ekonomi digital berjalan dengan lancar. Terkait dengan menyelenggarakan Sistem Elektroniknya, PSE harus secara aman dan andal sebagaimana dicantumkan pada Pasal 15 UU ITE.

Dengan menggunakan Sertifikat Keandalan, keandalan dan keamanan pelaku *e-commerce* terjamin karena telah dilakukan audit dari pihak ketiga *(third-party)* yaitu Lembaga sertifikasi keandalan. UU ITE mengatur penggunaan Sertifikat keandalan untuk menjamin perlindungan hukum terhadap privasi data dan keamanan sistem informasi dan transaksi elektronik.(Amirulloh, 2018) Pasal 1 angka 25 PP PSTE 71/2019 dinyatakan mengenai definisi Sertifikat Keandalan yaitu dokumen yang menyatakan bahwa pelaku usaha khususnya *e-commerce* menyelenggarakan Transaksi Elektroniknya dalam hal ini sudah lulus uji kesesuaian atau audit dari LSK atau Lembaga Sertifikasi Keandalan. Pelaku *e-commerce* yang menggunakan Sertifikat Keandalan membuktikan bahwa telah layak berusaha dalam melakukan *e-commerce* melalui audit atau penilaian, yang dibuktikan dengan pencantuman logo sertifikasi keandalan yaitu *trust mark* pada laman atau situs pelaku *e-commerce*.

Penggunaan Sertifikat Keandalan merupakan kewajiban bagi pelaku *e-commerce* sebagai Penyelenggara PMSE atau PPMSE, sebagaimana diatur pada Pasal 21 ayat (1) huruf e PP PMSE 80/2019. Sertifikat keandalan Keamanan Sistem Elektronik termasuk kedalam salah satu kategori sertifikat keandalan merujuk Pasal 76 ayat (1) PP PSTE 71/2019, menyatakan bahwa Lembaga Sertifikasi Keandalan menerbitkan Sertifikat Keandalan diantaranya kategorisari Kebijakan Privasi, Keamanan Sistem Elektronik, dan Registrasi Identitas yang menentukan level Sertifikat Keandalan tersebut.

Dalam penjelasan Pasal 76 ayat (1) PP PSTE 71/2019 dijelaskan bahwa jaminan keandalan dari Sertifikat Keandalan Keamanan Sistem Elektronik yaitu memastikan bahwa sistem manajemen keamanan informasi pelaku usaha terapkan merujuk kepada standar pengamanan dari sistem elektronik yang didasarkan kepada peraturan perundang-undangan. Standar pengamanan Sistem Elektronik tersebut mengacu terhadap pasal 24 ayat (2) PP PSTE 71/2019, yang menyatakan bahwa PSE memiliki kewajiban memiliki sistem pengamanan meliputi sistem serta prosedur dalam penanggulangan dan mencegah serangan dan ancaman yang mengakibatkan kegagalan, kerugian, atau gangguan.

Sertifikat Keandalan Keamanan Sistem Elektronik mengacu pada standar pengamanan sistem elektronik yang diatur pada peraturan kepala lembaga dalam pemerintahan pada bidang keamanan siber sebagaimana tercantum dalam pasal 24 ayat (4) PP PSTE, yaitu Badan Siber dan Sandi Negara. Berkaitan dengan Sertifikat Keandalan Keamanan Sistem Elektronik tersebut, BSSN mengeluarkan Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (selanjutnya disebut PBSSN 8/2020). BSSN sebagai lembaga pemerintah non-kementerian dalam kepentingan keamanan atau dalam hal ini keamanan sistem elektronik, berwenang menetapkan pemberlakuan SNI wajib, sebagaimana pasal 24 ayat (1) UU SPK 20/2014.

Pasal 2 PBSSN 8/2020 menyatakan bahwa sistem pengamanan dalam PSE dilaksanakan melalui Sistem Manajemen Pengamanan Informasi atau SMPI. Penerapan SMPI dilakukan oleh PSE PSE Lingkup privat dan Publik. *E-commerce* sebagai PSE lingkup privat dikategorikan ke dalam Sistem Elektronik berdasarkan asas risiko terbagi menjadi 3 kategori terdiri atas sistem elektronik: rendah, tinggi, dan strategis. Ketiga kategori Sistem Elektronik berdasarkan asas risiko tersebut memiliki standar wajib menggunakan SNI Wajib ISO/IEC 27001, yang tercantum dalam Pasal 9 PBSSN 8/2020.

Dalam hal ini penerapan SNI wajib ISO/IEC 27001 dibuktikan dengan Sertifikat SMPI. Sertifikat SMPI merupakan bukti yang diterbitkan oleh Lembaga Sertifikasi SMPI kepada PSE yang sudah memenuhi persyaratan. Sehingga, dapat dimengerti bahwa Sertifikat SMPI sebagai bukti penerapan SNI ISO/IEC 27001 dapat dimaknai sebagai sertifikat keandalan keamanan sistem elektronik yang adalah Sertifikat Keandalan yang menjamin sistem manajemen keamanan informasi pelaku *e-commerce* mengacu standar sistem pengamanan yang diatur oleh PBSSN 8/2020 yaitu SNI ISO/IEC 27001.

ISO/IEC 27001 merupakan standar *ISMS* atau *Information Security Management System* yang ditetapkan oleh IEC atau *International Electrotechnical Commission* dan ISO atau *International Organization for Standardization.*(Disterer, 2013) ISO/IEC 27001 disertifikasi dengan persyaratan yang harus dipenuhi sekaligus untuk meningkatkan kesadaran atas risiko dan kerentanan dari Sistem Elektronik. Di Indonesia, terdapat kasus-kasus serangan siber yang terjadi terhadap sistem elektronik pelaku usaha *e-commerce*, salah satunya kasus peretasan dan pencurian data pribadi konsumen Tokopedia pada bulan Mei tahun 2020. Kasus tersebut terjadi sebelum Tokopedia menggunakan ISO/IEC 27001 yang disertifikasi oleh Lembaga Sertifikasi Keandalan BSI (British Standards Institution) Group Indonesia. Saat ini, sesudah Tokopedia sebagai pelaku *e-commerce* telah menggunakan ISO/IEC 27001, apabila terdapat ancaman keamanan informasi seperti serangan siber pada sistem elektronik maka dapat diindentifikasikan lebih awal dan dapat segera ditangani.

Penerapan SNI ISO/IEC 27001 yang dibuktikan dengan Sertifikat Keandalan Keamanan Sistem Elektronik sangat penting bagi pelaku usaha *e-commerce* dalam mempersiapkan diri dan mengidentifikasi potensi kerentanan *(vulnabilitiy)* dalam sistem elektroniknya sebelum menghadapi gangguan dalam sistem elektronik. Berdasarkan hal-hal

tersebut, dikarenakan penggunaan Sertifikat Keandalan keamanan sistem elektronik telah menjadi kewajiban *pelaku e-commerce,* maka hal ini penting untuk dibahas mengenai bagaimana pelaksanaan kewajiban penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik oleh pelaku *e-commerce* di Indonesia dan mengenai bagaimana tangggung jawab pelaku *e-commerce* terkait penggunaan sertifikat keandalan keamanan sistem elektronik berdasarkan hukum siber di Indonesia.

METODE

Metode yuridis normatif digunakan pada penelitian ini, yaitu mengkaji hal-hal yang mempunyai sifat normative terutama yang terdapat dalam peraturan yang berlaku. Data sekunder adalah sumber data yang diperlukan dan digunakan dalam metode penelitian yuridis normatif yaitu anatara lain bahan hukum: tersier, primer, dan sekunder. Dalam bahan hukum data primer, yaitu bahan hukum yang memiliki kekuatan yang mengikat, yaitu: Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 Penyelenggaraan Sistem Transaksi Elektronik, Undang-Undang Nomor 20 Tahun 2014 Tentang Standardisasi dan Penilaian Kesesuaian, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, bahan hukum sekunder, seperti jurnal, artikel ilmiah, atau buku, dapat membantu peneliti menganalisis, menjelaskan, dan memahami bahan hukum primer. Bahan hukum tersier, misalnya rujukan elektronik, merupakan bahan hukum untuk membantu melengkapi, menjelaskan, atau mengarahkan bahan hukum primer atau bahan hukum sekunder.

HASIL DAN PEMBAHASAN

Pelaksanaan kewajiban penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik oleh pelaku *e-commerce* di Indonesia

Tujuan didirikannya Negara Kesatuan Republik Indonesia termaktub pada Pembukaan Undang Undang Dasar 1945, salah satunya adalah memajukan kesejahteraan umum. Terkait dengan negara kesejahteraan *(welfare state)* adalah sistem dimana negara melakukan tanggung jawab yang utama dalam hal memberikan keamanan secara ekonomi dan sosial penduduknya. Bahwa negara wajib mengusahakan kesejahteraan tercapai bagi masyarakatnya, salah satunya dengan menggunakan hukum untuk memperoleh kesejahteraan. Negara bertugas selain menjaga ketertiban dengan hukum, tetapi untuk memperoleh kesejahteraan bagi masyarakatnya dan kebijakan hukum harus berorietasi terhadap kesejahteraan rakyat.

Pasal 21 ayat (1) huruf e PP PMSE 80/2019 yang secara hukum memberikan kewajiban adanya sertifikat keandalan untuk mengamankan sistem elektronik yang dimiliki oleh pelaku *e-commerce* di indonesia agar dilaksanakan secara aman dan andal. Penggunaan sertifikasi keandalan keamanan sistem elektronik oleh pelaku *e-commerce,* akan berdampak kesejahteraan dalam bentuk keamanan sosial dalam melakukan transaksi elekronik konsumen akan tercapai. Dalam mengimplementasikan negara kesejahteraan, maka membutuhkan hukum dalam rangka mendorong dan mendukung pembangunan. Dalam hal ini sejalan dengan teori hukum pembagunan Mochtar Kusumaatmadja, dinyatakan bahwa istilah *as tool as social engineering* atau alat pembaharuan masyarakat (Kusumaatmadja, 2006).

Peran hukum dalam pembangunan, khususnya dalam bidang ekonomi adalah untuk menjamin bahwa perubahan itu terjadi teratur dengan adanya kebijakan yang jelas untuk setiap individu. Pasal 74 PP PSTE 71/2019 dinyatakan bahwa Sertifikat Keandalan memiliki tujuan melindungi konsumen dalam melakukan Transaksi Elektronik. Sejalan dengan tujuan sertifikat keandalan, pelaku *e-commerce* diharapkan menggunakan sertifikat

keandalan keamanan sistem elektronik agar tercapainya keandalan dan keamanan memberikan rasa aman bagi pengguna dalam bertransaksi elekronik.

Perkembangan TIK telah membentuk masyarakat informasi *(information society)*, yang mempunyai tingkat kebutuhan tinggi terhadap informasi sehingga yang menguasasi informasi akan mempunyai tingkat kesejahteraan lebih baik.(A. Amirulloh, 2016) Jaminan keamanan informasi *e-commerce* diperlukan oleh *Information society* agar menumbuhkan kepercayaan konsumen, dan terjadi peningkatan volume transaksi *e-commerce*. Keamanan informasi berpengaruh pada tercapainya tujuan transaksi elektronik yaitu berkembangnya perekonomian dan perdagangan secara lingkup nasional untuk meningkatkan kesejahteraan masyarakat, tercantum pada Pasal 4 huruf e UU ITE. Keamanan informasi dapat tercapai melalui sertifikat keandalan keamanan sistem elektronik.

Hukum memegang peran yang penting dalam mengarahkan kehidupan manusia, termasuk sejalan dengan *Pathetic dot theory*. Pentingnya sertifikat keandalan keamanan sistem elektronik dengan standar pengamanan SNI ISO/IEC 27001, telah di atur dalam pasal 9 PBSSN 8/2020 yang berdasarkan Kategori Sistem Elektronik didasarkan pada asas risiko. Berdasarkan asas risiko, sistem elekronik dikategorikan strategis, tinggi, dan rendah artinya ketentuan ini mengkonfirmasi bahwa sistem elektronik ini *vulnerability* untuk diserang. Dikarenakan berisiko, maka diwajibkan penggunaan ISO/IEC 27001 dalam PBSSN 8/2020 sebagai SNI Wajib. Dalam kepentingan keamanan sistem elektronik, BSSN berwenang menetapkan pemberlakuan SNI wajib berdasarkan BSSN berwenang menetapkan pemberlakuan SNI wajib berdasarkan dinyatakan pada pasal 24 ayat (1) UU SPK 20/2014.

BSSN memiliki kewenangan dalam melakukan penetapan pemberlakuan SNI secara wajib untuk kepentingan keamanan informasi yang mempertimbangkan risiko dari sistem elektronik. Risiko terhadap keamanan informasi ini dapat dilihat dari dampak *e-commerce* berpeluang memperbesar kemungkinan adanya *cybercrime* atau kejahatan dunia maya yang memberikan kurugian bagi konsumen. Pengaturan mengenai penggunaan sertifikat keandalan keamanan sistem elektronik berdampak melindungi konsumen dan mengurangi kerugian yang terjadi akibat sistem elektronik, dan memperkuat peran hukum dalam mengatur teknologi. Akibatnya sifat wajib dalam penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik dalam PP PMSE dan PBSSN 8/2020, memperkuat peran hukum dalam mengatur masyarakat mengenai melalui teknologi sejalan dengan *pathetic dot theory* (Amirulloh, 2023).

Pelaku *e-commerce* yang telah menggunakan Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001, maka telah mematuhi atau *comply* menjalankan kewajibannya. Pelaku *e-commerce* yang menggunakan SNI ISO/IEC 27001 diantaranya yaitu Tokopedia dan Shopee. Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001 tersebut disertifikasi oleh Lembaga Sertifikasi Keandalan yaitu Tokopedia disertifikasi oleh PT. BSI Group Indonesia dan Shopee disertifikasi oleh PT. TUV Rheinland Indonesia. Meskipun Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001 telah kewajiban bagi pelaku *e-commerce*, masih terdapat pelaku *e-commerce* yang tidak menggunakan SNI ISO/IEC 27001 diantaranya yaitu Blibli dan BukaLapak. Sehingga, pelaku e-commerce yang tidak menggunakan sertifikat keandalan keamanan sistem elektronik SNI Wajib ISO/IEC 27001 berpotensi melanggar ketentuan PP PMSE 80/2019, PBSSN 8/2020, UU SPK 20/2014.

Tanggung Jawab pelaku e-commerce terkait penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik di Indonesia

Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001 digunakan dalam rangka mencapai keandalan dan keamanan dalam penyelenggaraan sistem elektronik.

Kemudian, apabila penyelenggaraan sistem elektronik tidak diselenggarakan secara aman dan andal, maka pelaku *e-commerce* dapat dikenakan sanksi secara administratif, perdata, dan pidana. Lebih lanjutnya, sanksi Administrasif yang diberikan kepada pelaku *e-commerce* yang tidak menjalankan kewajiban penggunaan SNI ISO/IEC 27001, telah diatur dalam Pasal 37 ayat (2) PBSSN 8/2020 berupa teguran tertulis.

Sanksi Pidana terhadap pelaku *e-commerce* yang tidak menyelenggaraan sistem elektronik secara aman dan andal, dengan menerapkan SNI wajib ISO/IEC 27001 telah diaur dalam Pasal 65 UU SPK 20/2014 berupa pidana denda terbanyak yaitu tiga puluh lima miliar rupiah atau pidana penjara terlama yaitu lima tahun. Pelaku *e-commerce* yang menyelenggaraan sistem elektronik sehingga menimbulkan suatu kerugian maka, setiap orang dapat mengajukan gugatan sebagaimana terantum pada Pasal 38 UU ITE. Terdapat ketentuan bahwa setiap orang bisa mengajukan gugatan secara sendiri atau perwakilan dalam bentuk gugatan perdata ataupun arbitrase ataupun dengan lembaga penyelesaian sengketa alternatif. Penyelesaian sengketa dilakukan melalui non-litigasi didasarkan pada asas peradilan dilakukan secara cepat, biaya ringan, dan sederhana(Safira, 2017) pada Pasal 39 ayat (1) dan (2) UU ITE.

Pelaku *e-commerce* sebaiknya segera memperoleh sertifikat keandalan keamanan sistem elektronik agar sistem elektroniknya aman andal dan tidak merugikan konsumen, sehingga dibebaskan dari tanggung jawab hukum dengan memanfaatkan prinsip *safe harbor*. Prinsip *safe harbor* terkait dengan ketentuan dalam Pasal 11 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat serta Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2016 Tentang Batasan dan Tanggung Jawab Penyedia Platform dan Pedagang *(Merchant)* Perdagangan Melalui Sistem Elektronik *(E-Commerce)* yang Berbentuk *User Generated Content.* Pelaku *e-commerce* yang sudah *comply* dengan kewajiban Sertifikat Keandalan Keamanan Sistem elektronik, dapat memanfaatkan prinsip *safe harbor* sehingga mendapatkan perlindungan terkait pembatasan tanggung jawab. Seperti halnya Tokopedia dan Shopee yang sudah menerapkan kewajiban tersebut, dibatasi tanggung jawab tanggung jawab dikarenakan sudah *comply* terhadap kewajibannya.

Sertifikat Keandalan Keamanan Sistem Elektronik dengan standar SNI ISO/IEC 27001 sebagai pengaturan teknis mengenai penanggulangan dan pencegahan terhadap serangan dan ancaman yang menghasilkan kerugian, kegagalan, dan gangguan bagi konsumen dan pelaku e-commerce. Dengan adanya Sertifikat keandalan keamanan sistem elektronik, penyelenggara sistem elektronik khususnya *e-commerce* membantu menciptakan penyelenggaraan sistem elektronik menjadi aman dan andal sebagaimana diamanatkan dalam tujuan pemanfaatan transaksi elektronik pada UU ITE.

SIMPULAN

Belum semua pelaku *e-commerce* menggunakan Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001. Pelaku *e-commerce* yang telah menggunakan Sertifikat Keandalan Keamanan Sistem Elektronik disertifikasi oleh Lembaga Sertifikasi Keandalan, antara lain: Tokopedia disertifikasi oleh PT. BSI Group Indonesia dan Shopee disertifikasi oleh PT. TUV Rheinland Indonesia. Selain kedua pelaku *e-commerce* tersebut maka yang lain berpotensi melanggar PP PMSE, PBSSN 8/2020, dan UU SPK 20/2014 terkait kewajiban Sertifikat Keandalan Keamanan Sistem Elektronik SNI Wajib ISO/IEC 27001 bagi pelaku *e-commerce.* Pelaku *e-commerce* yang telah *comply* pada kewajiban penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik SNI ISO/IEC 27001 dibatasi tanggung jawab hukumnya berdasarkan ketentuan mengenai prinsip *safe harbor.*

Pelaku *e-commerce* yang tidak *comply* dengan kewajiban tersebut berpotensi melanggar hukum, maka pelaku *e-commerce* dapat dikenakan sanksi secara administratif, perdata, dan pidana. Mengingat pentingnya penggunaan Sertifikat Keandalan Keamanan Sistem Elektronik, pelaku *e-commerce* sebaiknya segera memperoleh sertifikat keandalan keamanan sistem elektronik agar sistem elektroniknya aman dan andal.

DAFTAR PUSTAKA

Amirulloh, A. (2016). *Hukum Teknologi Informasi dan Komunikasi (TIK) sebagai Hukum Positif di Indonesia dalam Perkembangan Masyarakat Global*. Unpad Press.

Amirulloh, M. & Muchtar, H. M. (2023). Implementation of Legal Certainty Principles and Pathetic Dot Theory in Relation to the Obligation of Privacy Trustworthiness Certification to Safeguard Consumer Personal Data in E-Commerce. *SRRN Journal*, 1–20.

Amirulloh, M. & Rachmadini, V. N. (2018). Legal Certainty in the Use of Certification of Trustworthiness by Indonesian E-Commerce Business. *Central European Journal of International and Security Studies*, *12*(4), 564–575.

Budhijanto, D. (2021). *E-Commerce Law: Fintech, Ekonomi Digital, dan Pelindungan Data Virtual*. Logoz Publishing.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *4*(2), 92–100.

Koloay, R. N. S. (2016). Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi. *Jurnal Hukum Unsrat* , *22*(5), 16–27.

Kusumaatmadja, M. (2006). *Konsep-konsep Hukum dalam Pembangunan*. Alumni.

Patel, H. B. (2021). E-Commerce Security Threats, Defenses Against Attacks and Improving Security. *International Journal Of Multidisciplinary Educational Research*, *9*(4), 172–182.

Ramli, T. S., Ramli, A. M., Budhijanto, D., & Permata, R. R. (2019). Prinsip-Prinsip Cyber Law Pada Media Over The Top E-Commerce Berdasarkan Transformasi Digital Di Indonesia. *Jurnal Legislasi Indonesia*, *16*(3), 392–398.

Safira, M. E. (2017). *Hukum Acara Perdata*. CV Nata Karya.