FUNGSI SERTIFIKASI ELEKTRONIK BAGI PELAKU USAHA DALAM TRANSAKSI PERDAGANGAN ELEKTRONIK

Siti Maisarah

Sekolah Tinggi Ilmu Ekonomi Cahaya Bangsa
E-mail: sarahmai09@yahoo.co.id

Abstract :

The aims of this research are to study and analyze the legal relation in electronic trading transaction using electronic certification and find the forms of electronic certification system which can be applied in electronic commercial transaction in Indonesia.

The presence of internet has become the supporting facility for the existence of sale and purchase agreement between the Seller and the Buyer. Since this is performed through internet world of course the Seller has the obligation to secure their situs web and at the same time to actualize the protection to the Buyer (consumer) who is entitled to comfort and security at the time of the process of electronic trading transaction. The Seller uses the services of Certification Authority to issue the Electronic Certificate with the type of Server Certificate called Secure Sockets Layer (SSL) Certificate in order to authenticate the identity of the situs web and to secure the space of the communication channel integrated to the said situs. This certifies that the situs web of shopping owned by the Seller has used a form of security. Based on that matter, it is deemed necessary the presence of domestic Certification Authority (owned by Indonesia) and the detailed legal regulations concerning the authorities of Certification Authority and the functions of SSL Certificate as one of implementations of Electronic Certificate as well as the obligation of the Seller to use the domestic SSL Certificate.

Keywords: *Seller, Buyer, Electronic Trade, Electronic Certificate*

Abstrak :

Tujuan penelitian ini adalah untuk mengkaji dan menganalisis hubungan hukum dalam transaksi perdagangan elektronik yang menggunakan sertifikasi elektronik serta menemukan bentuk sistem sertifikasi elektronik yang dapat diterapkan dalam transaksi perdagangan elektronik di Indonesia.

Hadirnya internet menjadi sarana pendukung adanya perjanjian jual beli antara Penjual dan Pembeli. Karena hal ini dilakukan dilakukan di dunia internet tentunya Penjual berkewajiban untuk mengamankan situs web mereka sekaligus wujud perlindungan terhadap Pembeli (konsumen) yang berhak atas kenyamanan dan keamanan saat proses transaksi perdagangan elektronik. Dengan Penjual menggunakan jasa layanan dari Otoritas Sertifikasi untuk penerbitan Sertifikat Elektronik berjenis Sertifikat Server bernama Sertifikat Secure Sockets Layer (SSL) untuk mengotentikasi identitas situs web serta mengamankan ruang saluran komunikasi yang terjalin dalam situs tersebut. Maka hal ini menyatakan bahwa situs web belanja milik Penjual tersebut telah menggunakan suatu bentuk pengamanan. Berdasarkan hal tersebut, maka perlunya Otoritas Sertifikasi dalam negeri (milik Indonesia) serta pengaturan hukum secara detail mengenai kewenangan Otoritas Sertifikasi dan fungsi Sertifikat SSL sebagai salah satu implementasi dari Sertifikat Elektronik serta kewajiban Penjual untuk menggunakan Sertifikat SSL dari dalam negeri.

Kata kunci: *Penjual, Pembeli, Perdagangan Elektronik, Sertifikat Elektronik*

PENDAHULUAN

Pengaturan jual beli di Indonesia dapat ditemui dalam Kitab Undang-Undang Hukum Perdata (KUHPer), kegiatan jual-beli didasari adanya "suatu persetujuan dengan mana pihak yang satu mengikatkan dirinya untuk menyerahkan suatu barang, dan pihak yang lain untuk membayar harga yang dijanjikan" (Pasal 1457 KUHPer).

Terkait jual beli, sebelumnya lebih identik dengan cara penjual dan pembeli bertemu secara langsung di suatu tempat dan metode pembayaran secara tunai. Sistem jual beli menjadi lebih modern karena dihubungkan oleh jaringan *Interconnection Networking* (Internet), disertai kemudahan sistem pembayaran di dunia maya, karena prosesnya menggunakan sistem elektronik maka terjadilah transaksi perdagangan elektronik.

Amanat Undang-Undang Nomor 7 Tahun 2014 Tentang Perdagangan (UUPerdagangan 7/2014) yaitu Pasal 65 ayat (1) bahwa "Setiap Pelaku Usaha yang memperdagangkan Barang dan/atau Jasa dengan menggunakan sistem elektronik …" dan pada Pasal 65 ayat (3) bahwa "Penggunaan sistem elektronik sebagaimana dimaksud pada ayat (1) wajib memenuhi ketentuan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik" yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE 19/2016).

Perlu diketahui bahwa dalam suatu Seminar Ekonomi Nasional di tahun 2018 bertema "*Quo Vadis* Ekonomi Digital Indonesia" Menteri Keuangan Sri Mulyani Indrawati menjelaskan bahwa jumlah pengguna internet di Indonesia telah mencapai lebih dari 100 juta pengguna namun nilai perdagangan transaksi perdagangan elektronik (*E-Commerce*) atau ekonomi digital masih rendah di kisaran 6%-9%. Dari sisi perdagangan yang menggunakan transaksi perdagangan elektronik itu nilainya masih 6%-9%.[1]

Bicara persoalan mengenai aspek keamanan dan legalitas dalam transaksi di internet sampai sekarang masih menjadi suatu persoalan. Hal ini disebabkan karena masalah keamanan sangat vital maka banyak perusahaan perangkat lunak seperti *Netscape* dan *Microsoft* telah membuat perangkat lunak yang mampu menjamin sekuriti transaksi perdagangan elektronik. Bukan hanya hal tersebut, tetapi muncul

[1] Kementerian Keuangan Republik Indonesia. *Nilai Perdagangan E-Commerce di Indonesia Masih Rendah*.2018.https://www.kemenkeu.go.id/publikasi/berita/nilai-perdagangan-e-commerce-di-indonesia-masih-rendah. Diakses pada tanggal 1/4/2018.

pula sertifikasi dan standarisasi sistem keamanan.[2]

Bicara mengenai sertifikasi, apabila ditelaah dalam UU ITE 19/2016 terdapat pihak Penyelenggara Sertifikasi Elektronik (PSrE) yaitu "badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik" (Pasal 1 angka 10). Pengertian Sertifikat Elektronik dapat ditemui pada Pasal 1 angka 9 UU ITE 19/2016 bahwa

> "sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik".

Dilihat dari isi pasal tersebut maka apabila digali lebih detail lagi menimbulkan pertanyaan mengenai pihak Sertifikasi (PSrE) yang mampu memberikan dan mengaudit Sertifikat Elektronik. Sertifikat Elektronik seperti apa dan apa fungsinya bagi Pelaku Usaha. Terkait persoalan mengenai aspek keamanan dan legalitas dalam transaksi di internet agar mampu menjamin sekuriti transaksi perdagangan elektronik, memunculkan suatu isu hukum mengenai keterlibatan pihak sertifikasi ini dalam kegiatan jual beli di dunia internet.

Dengan mengkaji dan menganalisis mengenai keterlibatan pihak Sertifikasi maka diharapkan dapat menggambarkan fungsi dari adanya pihak Sertifikasi dalam lingkup transaksi perdagangan elektronik khususnya bagi Pelaku Usaha. Karena dalam perdagangan di dunia internet, pelaku usaha tentunya memerlukan suatu tindakan yang bersifat preventif dan meminimalisir hal-hal negatif yang bisa terjadi di dunia internet. Sekaligus sebagai usaha melindungi keamanan dan kenyamanan pembeli selaku konsumen.

Kemudian, menimbulkan isu hukum lainnya yaitu untuk mendukung Sertifikasi melalui Sertifikat Elektronik di Indonesia. Hal ini tentunya memerlukan suatu sudut pandang, salah satunya untuk kepentingan dalam hal transaksi perdagangan elektronik di Indonesia, baik dari segi kejelasan aturan hukumnya maupun hal – hal yang bisa mendukung keberadaan sertifikasi di Indonesia.

PERUMUSAN MASALAH

Berdasarkan latar belakang masalah yang telah diuraikan, maka permasalahan yang akan dianalisis dalam penelitian ini, sebagai berikut :

1. Bagaimana hubungan hukum dalam transaksi perdagangan elektronik yang menggunakan sertifikasi elektronik?

[2] Abdul Halim Barkatullah. 2017. *Hukum Transaksi Elektronik Sebagai Panduan dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia*. Bandung: Nusa Media. hlm. 27

2. Bagaimana bentuk sistem sertifikasi elektronik yang dapat diterapkan dalam transaksi perdagangan elektronik di Indonesia?

PEMBAHASAN

A. Hubungan Hukum dalam Transaksi Perdagangan Elektronik yang Menggunakan Sertifikasi Elektronik

1. Para Pihak dalam Transaksi Perdagangan Elektronik

Berdasarkan namanya, Pasal 1319 KUHPer menyebutkan dua macam perjanjian, yaitu perjanjian bernama (nominaat) dan perjanjian tidak bernama (inominaat).[3] Perjanjian bernama terdapat dalam buku ketiga bab V hingga Bab XVIII KUHPer, perjanjian bernama (khusus) merupakan perjanjian yang memiliki nama sendiri, diatur dan diberi nama oleh pembentuk undang-undang berdasarkan tipe yang paling banyak terjadi sehari-hari.[4] Perjanjian jual beli termasuk ke dalam daftar perjanjian bernama dalam KUHPer.

Sistem Jual beli menjadi berkembang dengan jual-beli secara *online* atau perdagangan berbasis elektronik (*Electronic Commerce/E-Commerce*). Terkait para pihak dalam transaksi perdagangan elektronik, adanya "**Pelaku Usaha**" **(Penjual)**. Dalam Penjelasan Pasal 1 angka 3 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK 8/1999) tentang berbagai macam jenis Pelaku Usaha yaitu "perusahaan, korporasi, BUMN, koperasi, importer, pedagang, distributor, dan lain-lain". Dalam lingkup "*E-Commerce*", untuk jenis *Market Place*, seperti PT. Bukalapak dan PT. Tokopedia yang berbentuk Perseroan Terbatas (PT). Bukan berjenis *MarketPlace* misalnya seperti situs *8wood, Luna Habit* yang merupakan pelaku usaha yang bertindak sebagai produsen langsung yang bergerak dibidang industri mode pakaian.

Pembeli (konsumen) yaitu pihak yang melakukan pembelian produk (barang atau jasa) melalui pembelian di dunia internet, yang melakukan sistem pembayaran bisa dengan kartu kredit /debit. Dalam UUPK 8/1999 pada bagian penjelasan Pasal 1 angka 2 menyebutkan:

> Di dalam kepustakaan ekonomi dikenal istilah konsumen akhir dan konsumen antara. Konsumen akhir adalah pengguna atau pemanfaat akhir dari suatu produk, sedangkan konsumen

[3] Dadang Sukandar. 2017. *Panduan Membuat Kontrak Bisnis*. Jakarta: Visimedia, hlm 23.

[4] Dhanang Widijawan. 2018. *Dasar-Dasar Hukum Kontrak Bisnis Transaksi & Sistem Elektronik (UU ITE Perubahan No. 19/2016)*. Bandung: Keni Media, hlm 101.

antara adalah konsumen yang menggunakan suatu produk sebagai bagian dari proses produksi suatu produk lainnya. Pengertian konsumen dalam Undang-undang ini adalah konsumen akhir.

Dalam Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan. **Bank** dalam transaksi perdagangan elektronik berperan sebagai penyalur dana dari pihak pembeli kepada penjual dengan rincian sebagai berikut:

1. Tempat pelaku usaha (penjual) untuk membuka rekening miliknya agar dapat menampung aliran dana dari pembeli;
2. Sebagai ***acquier*** yaitu pihak perantara penagihan (antara penjual dan penerbit) dan perantara pembayaran (antara pemegang dan penerbit) dan sebagai perusahaan kartu kredit yang menerbitkan kartu (***issuer***).
3. Bank juga berperan sebagai *National Payment Gateway* bagi *cardholder* yang menggunakan kartu kredit (Peraturan Bank Indonesia No. 19/8/PBI/2017 tentang Gerbang Pembayaran Nasional).

Certification Authority **(CA)** atau pihak Sertifikasi Elektronik/Otoritas Sertifikasi. Otoritas ini menerbitkan jasa layanan sertifikat elektronik atau sertifikat digital. Dalam penelitian ini terkait sertifikat elektronik yang dapat dimiliki oleh pelaku usaha (penjual). Perlu diketahui bahwa tidak semua Pelaku Usaha menggunakan jasa dari pihak CA.

Pihak *Internet Service Provider* yaitu **Penyedia Jasa Internet (PJI)** dan Pengembang (*intellectual agent*) :

a. Penyedia Jasa Internet (ISP)
   Pemilik ruang elektronik yang disebut *website/keybase*.
b. Pengembang
   Pelaku bisnis yang mengadakan e-kontrak langsung dengan ISP.[5]

Pihak **Jasa Pengiriman** misalnya seperti JNE, J&T, POS Indonesia, Tiki, dan *Go-Send*. Pihak **Pemerintah** berperan dalam hal menyusun dan mensahkan berbagai aturan yang bisa mendukung keberadaan transaksi perdagangan elektronik di Indonesia. Misalnya memberikan perlindungan hukum terhadap pelaku usaha dan konsumen.

Terkait metode pembayaran yang biasanya disediakan pelaku usaha adalah pembayaran tunai melalui kurir saat pengiriman (*cash on delivery* /COD). Namun, sistem pembayaran dengan cara seperti itu belum bisa dikatakan sepenuhnya transaksi perdagangan elektronik. Karena apabila transaksi perdagangan

[5] Mariam Darus Badrulzaman, dkk. 2001. *Kompilasi Hukum Perikatan*. Bandung: PT. Citra Aditya Bakti, hlm. 281-282.

elektronik seutuhnya metode pembayaran yang digunakan juga *online*. Selama ini *mobile payment* dikenal paling banyak adalah dari produk perbankan yang biasa dikenal dengan nama *Mobile Banking*.

2.Penggunaan Sertifikasi Elektronik dalam Sistem Perdagangan Elektronik

Sertifikat elektronik atau sertifikat digital yang berjenis *server certificate* atau sertifikat *Secure Sockets Layer* (SSL). Pada praktiknya sertifikat ini diberikan oleh suatu Otoritas Sertifikasi atau *Certification Authority* (CA). Penggunaan jenis sertifikat digital untuk membangun keamanan situs web, *server certificate* digunakan untuk membuktikan identitas server seperti web yang merupakan salah satu penggunaan sertifikat server yang bernama sertifikat SSL.[6]

Pada saat melakukan transaksi di internet, sertifikat digital merupakan sertifikat elektronik yang menetapkan keabsahan. Sertifikat ini berisikan nama, nomor serial, tanggal kadaluwarsa, tanda tangan pengguna, dan tanda tangan pihak yang mengeluarkan sertifikat sehingga pihak penerima dapat memverifikasi kebenarannya.[7] Keterangan tersebut mengisi tampilan sertifikat elektronik. Namun, dibalik tampilan sertifikat elektronik terpasang SSL pada situs web dagang tersebut.

SSL merupakan teknologi keamanan standar global yang digunakan oleh jutaan bisnis *online* dan individu untuk mengurangi risiko informasi yang bersifat sensitif (misalnya, nomor kartu kredit, nama pengguna, kata sandi, *email*, dll) dari pencurian atau perusakan oleh peretas dan pencuri identitas. Pada intinya, SSL memungkinkan dilakukannya "komunikasi" pribadi antara dua pihak yang ditujukan. Untuk menciptakan koneksi yang aman ini, suatu sertifikat SSL (yang juga disebut sebagai "sertifikat digital") diinstal pada server web dan melayani dua fungsi:

a. Sertifikat ini mengotentikasi identitas situs web (menjamin pengunjung bahwa situs web tersebut bukan merupakan situs web palsu)
b. Sertifikat ini mengenkripsi data yang sedang dikirim [8]

[6] Direktorat Jenderal Aplikasi Informatika. *Sivion-Solusi Identitas Digital Terpercaya*. 2016. https://aptika.kominfo.go.id/index.php/artikel/134-sivion-solusi-identitas-digital-terpercaya. Diakses pada tanggal 1/7/2018.

[7] Jonathan Sarwono dan K. Prihartono AH. 2012. *Perdagangan Online : Cara Bisnis Di Internet*. Jakarta: PT Elex Media Komputindo. hlm., 55.

[8] VeriSign, Inc. *Semua yang Perlu Anda Ketahui Tentang Sertifikat SSL*. https://www.verisign.com/in_ID/website-presence/website-optimization/ssl-certificates/index.xhtml. Diakses pada tanggal 1/7/2018.

Jika penggunaan sertifikat elektronik (sertifikat digital) yang berjenis *server certificate* atau sertifikat SSL dalam transaksi perdagangan elektronik dikaitkan dengan kepastian hukum, maka terdapat dua hal yang menyangkut dengan kepastian hukum dalam hal ini:

1. Pertama, dengan adanya otentikasi identitas situs web maka kepastian hukum identitas situs web belanja *online* milik pelaku usaha tersebut jelas, yang mana juga berimbas terhadap calon pembeli bahwa situs yang disinggahinya bukan situs palsu. Namun, dengan catatan bukan berarti situs milik pelaku usaha yang tidak menggunakan *server certificate* atau sertifikat SSL ini adalah situs palsu. Hanya saja, kualitas keamanan situsnya kurang maksimal yang otomatis juga berpengaruh terhadap kualitas usaha milik pelaku usaha tersebut. Karena sebelum sertifikat ini diberikan si pelaku usaha tersebut identitasnya harus jelas karena akan diperiksa terlebih dahulu oleh pihak berwenang yang bisa menerbitkan sertifikat tersebut.
2. Kedua, dengan adanya enkripsi data maka saat terjadinya pertukaran data yang terjadi di dalam situs tersebut terbilang keamanannya maksimal, terkait kepastian hukum bagi pelaku usaha sekaligus pembeli mengenai keamanan data mereka.

Berbagai kegiatan yang dilakukan di dalam situs web tersebut misalnya saat seseorang memasuki suatu situs dagang dan memutuskan untuk berbelanja disitus tersebut biasanya situs tersebut terlebih dahulu meminta untuk mendaftarkan diri dengan membuat akun. Dengan memasukkan data-data pribadi dan membuat *password* milik sendiri untuk kemudahan *log in* saat ingin berbelanja. Ketika *log in* ke dalam akun yang sudah dibuat tadi dengan memasukkan nama dan *password* yang telah dibuat terdapat ruang saluran komunikasi yang terjadi, teknologi sertifikat SSL yang dimiliki situs tersebut akan mengamankan ruang saluran tersebut dari hal-hal negatif yang bisa terjadi di dunia internet. Agar saat pembeli *log in* ke dalam akunnya proses tersebut aman dari pihak yang tidak berkepentingan. Jadi, data-data pembeli terbilang aman.

Pentingnya data pribadi dapat dikutip dari pernyataan CEO Tokopedia, Wiliam Tanuwijaya yang memastikan bahwa data pribadi pengguna layanannya dijamin aman

dan dirahasiakan. Tak ada satu pun data yang dioper ke pihak ketiga. Begitu pula CEO Bukalapak, Achmad Zaky bahwa situs dan aplikasi Bukalapak menggunakan protokol HTTPS sehingga setiap data yang dikirimkan oleh pengguna sudah dienkripsi. Cara tersebut membuat data tidak bisa dibaca oleh pihak lain, baik melalui jaringan seluler atau WiFi publik.[9]

Kemanfaatan dan kepastian hukum dapat menjadi sesuatu yang beriringan. Karena itu sesuai dengan bunyi Pasal 4 huruf e UU ITE 11/2008 bahwa "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi".

Dalam proses pembayaran secara elektronik oleh pembeli kepada sistem yang menangani masalah pembayaran pada situs web transaksi perdagangan elektronik. Untuk kemudian dilakukan kontak dengan layanan yang diberikan oleh Bank (yang digunakan oleh pembeli untuk melakukan pembayaran). Pada proses pembayaran elektronik ini, di belakang layar diaktifkan sejumlah teknologi keamanan (SSL), untuk menjamin agar proses pembayaran berlangsung dengan aman dan nyaman.[10]

Cara untuk melihat tampilan Sertifikat SSL pada suatu situs *online*:

1. Pertama, saat membuka sebuah situs transaksi perdagangan elektronik dapat dilihat pada bagian pojok paling atas. Apabila aman akan terdapat tanda gembok *(secure*) dan https:/ / ;
2. Kedua, klik *secure* kemudian klik valid akan langsung terlihat tampilan sertifikat elektronik. Tertera pada sertifikat tersebut pada bagian general untuk mengetahui sertifikat diterbitkan untuk siapa (*issued to*), sertifikat diterbitkan oleh *(issued by*), tanggal valid sertifikat tersebut (*valid from*). Kemudian bisa diklik bagian details untuk melihat bentuk tanda tangan elektronik (*signature*), dan juga ada bagian certification path untuk melihat keterangan proses verifikasi atau validasi jalur.

Gambar 1.1 Contoh Peringatan untuk Situs Web tanpa menggunakan SSL
Sumber: https://www.123-reg.co.uk/ssl-certificates/

[9] Yoga Hastyadi Widiartanto. *Bukalapak dan Tokopedia Jelaskan Aplikasinya yang LacakDataPengguna*.2016.https://tekno.kompas.com/read/2016/11/02/13020077/bukalapak.dan.tokopedia.jelaskan.aplikasinya.yang.lacak.data.pengguna. Diakses pada tanggal 1/7/2018.

[10] I Putu Agus Eka Pratama. 2014. *Komputer dan Masyarakat*. Bandung: Informatika, hlm 157.

Keterangan Gambar diatas :

a. Status info tidak aman, yang berarti *website* tersebut tidak menggunakan koneksi pribadi atau dapat juga halaman tersebut memiliki tautan yang mengarah ke halaman HTTP (tidak aman).

b. Status info tidak aman atau berbahaya, info ini merupakan penandaan bahwa situs web tersebut ditandai berpotensi berbahaya. Google telah melakukan penerapan untuk semua situs web yang tidak memiliki sertifikasi SSL akan ditampilkan tanda segitiga-merah yang berarti 'tidak aman' yang pada saat ini dapat dilihat pada *browser Chrome*.[11]

3. Hubungan Perikatan Para Pihak dalam Transaksi Perdagangan Elektronik dengan Menggunakan Sertifikasi Elektronik

Dalam kegiatan jual beli yang dilakukan di dunia internet maka pelaku usaha (penjual) terkait situs belanja *online* miliknya memerlukan suatu perlindungan yang bermanfaat di dunia internet dan sah secara hukum. Hak dan kewajiban masing-masing pihak haruslah dilindungi secara hukum. Dikarenakan semua hal ini terjalin di dunia internet yang termasuk jaringan publik yang bisa dimasuki pihak yang tidak beritikad baik atau berbagai virus jaringan.

Jika dikaitkan dengan perlindungan hukum, keberadaan hukum dalam masyarakat merupakan suatu sarana menciptakan ketentraman dan ketertiban masyarakat. Sehingga dalam hubungan antara anggota-anggota masyarakat, hak-hak dan kewajibannya dilindungi oleh hukum. Hukum tidak lain adalah norma atau kaidah perlindungan kepentingan manusia.[12]

Fokus dalam penelitian ini adalah Pelaku Usaha dengan Konsumen (*Business to Consumer*/BtoC) yang termasuk dalam lingkup privat (Pasal 40 ayat 3 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE 82/2012). Walau dalam hal ini, subjek utamanya adalah penjual dan pembeli, namun, untuk menjelaskan 'hubungan perikatan para pihak dalam transaksi perdagangan elektronik dengan menggunakan sertifikasi elektronik', melibatkan peran pihak lainnya yang membantu terselenggaranya suatu proses transaksi perdagangan elektronik.

[11] IndonesiaGo Digital. *Fungsi Serta Pentingnya Sertifikasi SSL (HTTPS) Bagi Website Anda*. 2017. https://indonesiago.digital/sertifikasi-ssl-https-bisnis-anda/. Diakses pada tanggal 5/7/2018.

[12] Sudikno Mertokusumo. 2003. *Mengenal Hukum Suatu Pengantar*. Yogyakarta: Liberty, hlm 39.

Maka uraiannya dapat dijelaskan dari hal **pertama**, Pelaku Usaha (Penjual) Pemilik Situs Dagang *Online* bekerjasama dengan *Internet Service Provider* atau Penyedia Jasa Internet (PJI). PJI adalah pihak perusahaan yang menyediakan layanan sambungan internet kepada pelanggan agar bisa menikmati jaringan internet, pendaftaran nama domain, dan juga *hosting*.

Kedua, mengenai hubungan hukum pelaku usaha (Penjual) dengan Pembeli (konsumen). Penjual berkewajiban untuk mengamankan setiap kegiatan yang dilakukan dalam lingkup situsnya untuk melindungi usahanya di dunia internet. Melalui Otoritas Sertifikasi/*Certification Authority* (CA) yang dapat memberikan sertifikat elektronik atau sertifikat digital berjenis Sertifikar Server bernama Sertifikat *Secure Sockets Layer* (SSL) sebagai bentuk bukti bahwa Penjual sudah menggunakan pengamanan untuk usaha jual beli miliknya di dunia internet.

Dalam hal kerjasama dengan didasari oleh perjanjian jual beli namun dalam hal tentang layanan jasa pengamanan "perjanjian jual beli jasa pengamanan". Dari hubungan hukum tersebut mengakibatkan adanya hak dan kewajiban apabila dilihat dari alur perjanjiannya yaitu :

1. Pihak pelaku usaha berkewajiban untuk menjalani serangkaian pemeriksaan identitas pelaku usaha serta usahanya dari pihak Sertifikasi dan membayarkan sejumlah biaya yang sudah ditentukan oleh pihak CA untuk bisa mendapatkan Sertifikat SSL.
2. Pihak CA atau Otoritas Sertifikasi berhak untuk menerbitkan sertifikat elektronik, serta berhak mencabut atau menonaktifkan sertifikat elektronik milik pengguna apabila sudah dalam batas valid dari batas waktu yang sudah ditentukan sebelumnya serta menetapkan dan menerima biaya atas jasa penerbitan sertifikat elektronik.

Ketiga, dalam hal untuk memudahkan Pembeli (*card holder*) melakukan proses pembayaran maka Penjual melakukan kerjasama dengan pihak Bank sebagai penerima kuasa. Hubungan hukum yang terjalin antara pihak pelaku usaha dengan pihak Bank yang merupakan pemberian kuasa khusus. Bank berperan sebagai *National Payment Gateway* bagi Pembeli yang menggunakan kartu kredit, yang diatur dalam Peraturan Bank Indonesia Nomor 19/8/PBI/2017 tentang Gerbang Pembayaran Nasional.

Keempat, Pelaku Usaha melakukan perjanjian kerjasama dengan jasa pengiriman. Berdasarkan isi Pasal 1476 KUHPer "Biaya penyerahan dipikul oleh penjual, sedangkan biaya pengambilan dipikul oleh pembeli, kecuali kalau diperjanjikan sebaliknya". **Kelima**, ketika pelaku usaha (Penjual) selaku pemilik situs belanja *online* dengan pembeli 'konsumen' (*card holder*) melakukan perbuatan hukum yaitu melakukan perjanjian jual beli yang merupakan sumber dari perikatan. Diawali dari adanya penawaran dan penjualan dari pelaku usaha dan pembelian dari pembeli yang melahirkan perjanjian jual beli secara *online* yang kemudian menyebabkan adanya hubungan hukum dengan jenis pelaku usaha dengan konsumen (BtoC) menyebabkan hadirnya kewajiban dan hak masing-masing pihak. Pembeli berkewajiban untuk melakukan pembayaran atas barang yang sudah dipilihnya untuk dibeli. Kewajiban Penjual yaitu apabila konfirmasi pembayaran sudah diterima oleh penjual maka suatu kewajiban bagi penjual untuk segera mengirimkan barang.

Keenam, perjanjian penerbitan kartu antara *Issuer* (bank/lembaga bukan bank) dengan pemegang kartu (*card holder*) yang mengakibatkan hubungan hukum dengan *card holder* sebagai sarana si pembeli, untuk dapat memiliki kartu debit/kartu kredit yaitu perjanjian antara *issuer* dengan *card holder*, yang nantinya digunakan sebagai sumber untuk melakukan pembayaran.

B. Bentuk Sistem Sertifikasi Elektronik Yang Dapat Diterapkan Dalam Transaksi Perdagangan Elektronik Di Indonesia

1. Peraturan Hukum di Indonesia yang Mengatur Sertifikasi Elektronik

Dimulai dari UU ITE 19/2016 yaitu pada Pasal 1 angka 9 UU ITE 19/2016 bahwa:

> Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

Diawali dari unsur yang **pertama**, bahwa Sertifikat Elektronik bersifat elektronik. Dalam "Kamus Bahasa Indonesia" Sertifikat adalah "surat keterangan dari orang berwenang dan dapat digunakan untuk keperluan tertentu".[13] Dalam hal ini sertifikat tidak berbentuk fisik (akta atau surat),

[13] Bambang Marhiyanto. *Kamus Lengkap Bahasa Indonesia*. Surabaya: Media Centre, hlm 565.

namun bersifat elektronik artinya sertifikat tampilannya hanya dapat dilihat di dunia maya atau di dunia internet.

Unsur **kedua**, yaitu terdapat Tanda Tangan Elektronik. Tanda tangan elektronik seperti dalam UU ITE 19/2016 Pasal 1 angka 12 bahwa :

> Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

Apabila mengingat kembali tampilan dari Sertifikat Elektronik yang ada pada situs web, disana terdapat bagian tanda tangan (*signature*) yang berwujud algoritma, bukan tanda tangan seperti umumnya yang berwujud fisik diatas kertas. Namun, berupa kode-kode huruf dan angka. Milik siapa tanda tangan tersebut? Tentunya Penanda Tangan merupakan "subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik" (Pasal 1 angka 13 UU ITE 19/2016). Karena bicara mengenai Sertifikat untuk kepentingan usaha situs belanja *online* yaitu Sertifikat Server bernama Sertifikat SSL maka tanda tangan elektronik hanya digunakan di salah satu tahapan protokol untuk Sertifikat SSL.

Unsur **ketiga**, Sertifikat Elektronik memuat "identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik" (Pasal 1 angka 9 UU ITE 19/2016). Apabila dilihat pada tampilan sertifikat pada situs web milik penjual maka dapat terlihat keterangan yang menunjukkan siapa PSrE atau CA yang mengeluarkan sertifikat tersebut, misalnya '*Issued by: Digicert'* dan kepada siapa sertifikat tersebut diberikan misalnya '*Issued to*: *.bukalapak.com.' Jadi, dari keterangan tersebut terlihat identitas masing–masing subjek hukum statusnya sebagai apa dalam Transaksi Elektronik tersebut.Transaksi elektronik bukan hanya diidentikkan dengan transaksi berupa uang, namun juga bisa hal yang lain selagi itu merupakan perbuatan hukum yang menggunakan sarana elektronik. Misalnya transaksi berupa informasi elektronik antara pihak yang mengeluarkan sertifikat dengan pihak yang menerima sertifikat tersebut (*Issued by dan Issued to*).

Unsur **keempat**, yaitu mengenai Sertifikat Elektronik yang dikeluarkan oleh PSrE. Sesuai bunyi Pasal 1 angka 10 UU ITE 19/2016 dijelaskan bahwa

PSrE itu berbentuk badan hukum artinya bisa publik (pemerintah) atau privat (swasta). PSrE adalah pihak yang mengeluarkan sertifikat elektronik, yaitu pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik. Sebelum pihak PSrE mengeluarkan/memberikan Sertifikat Elektronik kepada calon pemegang Sertifikat Elektronik maka sebelumnya PSrE menerima pendaftaran dari calon pemegang Sertifikat Elektronik.

Dari rangkaian penjelasan diatas, gambaran Sertifikat Elektronik apabila diambil dari isi Pasal 1 angka 9 UU ITE 19/2016, pada dasarnya sudah dapat menggambarkan tampilan Sertifikat Elektronik secara umum, baik itu tampilan jenis Sertifikat Elektronik untuk kepentingan Tanda Tangan Elektronik dan tampilan jenis Sertifikat Elektronik untuk kepentingan Situs Web (Sertifikat SSL). Namun, lebih detail mengenai manfaat atau kegunaannya belum mengarahkan ke sertifikat server yang bernama Sertifikat SSL. Apabila dipandang lebih detail masih kurang menunjukkan keberadaan Sertifikat Server (sertifikat SSL) yang juga merupakan salah satu fungsi dari Sertifikat Elektronik. Karena Sertifikat Elektronik bukan hanya terkait kepentingan Tanda Tangan Elektronik untuk menandatangani Dokumen Elektronik, namun juga untuk Sertifikat Server (sertifikat SSL).

Sertifikat Elektronik yang ditujukan untuk keterangan identitas diri sendiri secara pribadi yang diwakilkan dalam bentuk Tanda Tangan Elektronik (pengabsahan dokumen kerja, perusahaan) melalui tanda tangan digital bersertifikat sebagai identitas digital. Hal ini didukung melalui UU ITE dan PP PSTE yang mengatur secara detail untuk kepentingan ini. Sedangkan, untuk kepentingan identitas situs web terkait usaha yaitu sertifikat SSL hanya secara umum saja.

PP PSTE Penjelasan Pasal 54 Ayat (1) sangat jelas menunjukkan dengan detail mengenai Tanda Tangan Elektronik, sebagai berikut:

> Akibat hukum dari penggunaan Tanda Tangan Elektronik tersertifikasi atau yang tidak tersertifikasi berpengaruh terhadap kekuatan nilai pembuktian. Tanda Tangan Elektronik yang tidak tersertifikasi tetap mempunyai kekuatan nilai pembuktian meskipun relatif lemah karena masih dapat ditampik oleh yang bersangkutan atau relatif dapat dengan mudah diubah oleh pihak lain. Dalam praktiknya perlu diperhatikan rentang kekuatan nilai pembuktian dari Tanda Tangan Elektronik yang

bernilai pembuktian lemah, seperti tanda tangan manual yang dipindai (*scanned*) menjadi Tanda Tangan Elektronik sampai dengan Tanda Tangan Elektronik yang bernilai pembuktian paling kuat, seperti Tanda Tangan Digital yang diterbitkan oleh penyelenggara sertifikasi elektronik yang tersertifikasi.

Patut diketahui Sertifikat Elektronik berjenis Sertifikat Server bernama Sertifikat SSL ini menjadi salah satu kategori penilaian dari Lembaga Sertifikasi Keandalan (LSK) kepada Pelaku Usaha apabila ingin lolos dari penilaian LSK dan mendapatkan logo *trustmark*. Ketentuan lanjutan mengenai LSK juga terdapat pada PP PSTE 82/2012 karena sesuai amanat Pasal 10 ayat (2) UU ITE 11/2008. Dalam PP PSTE tersebut dijelaskan pada Pasal 1 angka 25 bahwa Sertifikat Keandalan merupakan "dokumen yang menyatakan Pelaku Usaha yang menyelenggarakan Transaksi Elektronik telah lulus audit atau uji kesesuaian dari Lembaga Sertifikasi Keandalan".

Dalam ketentuan Penjelasan Pasal 68 ayat (1) PP PSTE bahwa Sertifikat Keandalan yang diterbitkan oleh LSK meliputi kategori :

a. pengamanan terhadap identitas (*identity seal*) merupakan SK yang jaminan keandalannya sebatas pengamanan bahwa identitas Pelaku Usaha adalah benar …… ;
b. Pengamanan terhadap pertukaran data (*security seal*) merupakan SK yang jaminan keandalannya memberikan kepastian bahwa proses penyampaian atau pertukaran data melalui situs web Pelaku Usaha dilindungi keamanannya dengan menggunakan teknologi pengamanan proses pertukaran data (contoh: **protokol SSL/secure socket layer**). Sertifikat Keandalan ini menjamin bahwa terdapat sistem pengamanan dalam proses pertukaran data yang telah teruji;
c. Pengamanan terhadap kerawanan (*vulnerability seal*) ….. ;
d. Pemeringkatan konsumen (*consumer rating seal*) ….. ;
e. Pengamanan terhadap kerahasiaan Data Pribadi (*privacy seal*) …...

Gambar 1.2 Contoh Sertifikat Keandalan dan Sertifikat Elektronik
Sumber : Ekosistem Penyelenggaraan Sertifikat Elektronik Dalam Sistem Perdagangan Elektronik Oleh Ahmad Budi Setiawan

2. Bentuk Sistem Sertifikasi Elektronik di Beberapa Negara

Dibawah aturan *Electronic Transaction Act* (ETA) Singapura 2010, pemerintah Singapura mempunyai *Certification Authority* bernama Netrust yang mampu menerbitkan Sertifikat Elektronik untuk Server (sertifikat SSL).

Netrust menyediakan untuk individu, bisnis dan organisasi pemerintah dengan identifikasi *online* lengkap dan infrastruktur keamanan untuk memungkinkan transaksi elektronik yang aman. Selain penyediaan sertifikat. Sebagai bukti untuk bisnis yang efisien dan proses operasional dalam Netrust, Pengawas CA yaitu *Infocomm Development Authority* (IDA) memberikan Lisensi CA (sekarang Akreditasi) ke Netrust pada Juni 2001. Netrust menerbitkan serangkaian sertifikat digital untuk aplikasi *online* termasuk akses aman ke aplikasi pemerintah, Internet *banking*, jaringan pribadi virtual dan akses aman ke portal intranet. Sebagai CA Terakreditasi, pihak-pihak yang mengandalkan sertifikat Netrust menikmati manfaat pembuktian dan pengguna dijamin akan legalitas dan keamanan transaksi mereka.[14]

Pada Netrust, Sertifikat Server Web SSL memungkinkan penyedia layanan untuk menggunakan protokol SSL untuk otentikasi server web dan enkripsi data. Sertifikat Server Web SSL Netrust adalah sertifikat X.509 v3 yang memenuhi standar yang mampu mendukung kemampuan enkripsi sesi 256-bit dan 128-bit penuh dan diakui oleh browser web terkemuka seperti *Internet Explorer (IE) dan Mozilla Firefox, Google Chrome , Safari*.[15]

Pada Amerika Serikat (AS), Pemerintah mengizinkan sektor swasta untuk menerapkan kebijakan privasi mereka sendiri. Salah satu cara yaitu diadopsi oleh pedagang di Internet yaitu menerapkan layanan otentikasi Sertifikat Elektronik untuk Server (sertifikat SSL) melalui CA/Otoritas Sertifikasi seperti *Digicert* dan *Verisign*.

Pemerintah AS mengizinkan sektor swasta untuk menerapkan kebijakan privasi mereka sendiri. Menurut AS, penjual dalam transaksi perdagangan elektronik harus

[14] Netrust Pte Ltd. https://www.netrust.net/about/. Diakses pada tanggal 26/7/2018.

[15] *Ibid*

mengembangkan model pengaturan mandiri (*self-regulation*) untuk mendapatkan kepercayaan konsumen. *Federal Trade Commission* (FTC) yaitu sebuah agen federal independen yang bertugas melindungi kepentingan ekonomi bisnis dan konsumen di AS, telah mempromosikan *self-regulation* untuk penjual sebagai bagian penting dari perlindungan hukum bagi konsumen. *Self-regulation* ini sejalan dengan prinsip-prinsip yang ditetapkan dalam Peraturan Global Elektronik (*Global Electronic Business Work Regulation*) yang dipromosikan oleh Presiden Clinton dan Wakil Presiden Gore untuk mencegah peraturan pemerintah yang menghambat investasi teknologi tinggi.[16]

Self-regulation otonom lain yang diadopsi oleh pedagang di Internet adalah menerapkan layanan otentikasi, seperti *Verisign*. Layanan ini mengontrol identitas situs web dan menyakinkan konsumen bahwa informasi seperti nomor kartu kredit akan tetap aman untuk menghindari pihak ketiga memperoleh informasi.[17]

3. Perspektif Penggunaan Sertifikasi Elektronik dalam Perdagangan di Indonesia

Perspektif penggunaan sertifikasi elektronik dalam perdagangan di Indonesia maka hal **pertama**, bicara mengenai pengaturan mengenai pihak Sertifikasi (PSrE) dan Sertifikat Elektronik yang dihasilkannya yang bermanfaat untuk Pelaku Usaha transaksi perdagangan elektronik yaitu melalui layanan suatu lembaga sertifikasi seperti *Certification Authority* (CA). Kenapa hal tersebut perlu diatur detail secara hukum? Pertama, akan dianalogikan melalui Tanda Tangan Elektronik yang mempunyai Sertifikat Elektroniknya sendiri. Sertifikat tersebut untuk menunjukkan kepemilikan Tanda Tangan Elektronik seseorang (identitas penandatangan yang tersertifikasi). Manfaat tanda tangan elektronik tersebut adalah untuk pengesahan suatu dokumen elektronik seperti surat izin pengajuan cuti, kontrak kerjasama dan lain-lain yang bersifat elektronik.

Ketika penjelasan Sertifikat Elektronik untuk Tanda Tangan Elektronik tadi disandingkan dengan Sertifikat Elektronik untuk menunjukkan penggunaan Sertifikat SSL yang juga punya tampilan sertifikat layakmya sertifikat untuk

[16] Abdul Halim Barkatullah dan Djumadi. *Does self-regulation provide legal protection and security to e-commerce consumers?*. 2018. Artikel dalam "Jurnal Elsevier". May, hlm. 96.

[17] *Ibid*, hlm. 97.

Tanda Tangan Elektronik. Diperlukan pengaturan fungsi yang lebih detail lagi karena lebih dari sekedar menunjukkan identitas penandatangan yang tersertifikasi. Namun, juga untuk menyatakan penggunaan Sertifikat SSL dari jasa layanan *Certification Authority* (Otoritas Sertifikasi).

Padahal manfaat dari Sertifikat SSL ini penting, intinya sebagai tanda bahwa situs pelaku usaha sudah bersertifikat dari Otoritas Sertifikasi dan tentunya koneksi saluran komunikasi yang sudah diamankan oleh Otoritas Sertifikasi. Sementara ini, Sertifikat SSL yang dipakai Pelaku Usaha di Indonesia banyak yang berasal dari Otoritas Sertifikasi milik asing. Hal ini mengingatkan pada waktu dulu, saat Indonesia belum mempunyai fasilitas Tanda Tangan Elektronik dari dalam negeri sendiri.

Patut diingat, kegiatan perdagangan yang dilakukan melalui perantara dunia maya/internet, artinya si Pelaku Usaha tidak terlihat secara fisik dan tidak bisa dilakukan pengawasan keamanan layaknya perdagangan secara konvensional. Karena itu diperlukan suatu pihak yang mampu mencek atau memeriksa Si Pelaku Usaha tersebut seperti Lembaga Sertifikasi Keandalan (LSK) yang sudah dibahas sebelumnya, namun tentunya bukan hanya sebatas menilai sang Pelaku Usaha tersebut, namun juga pihak yang mampu menerbitkan Sertifikat Elektronik berjenis Sertifikat Server untuk Web bernama Sertifikat SSL seperti *Verisign, Digicert,* dan *Comodo*.

Otoritas Sertifikasi merupakan elemen-elemen yang seharusnya menyatu dalam satu naungan, yaitu terdiri dari tim penilai dan penjamin keandalan Pelaku Usaha, sekaligus penyedia layanan sertifikat elektronik berjenis sertifikat SSL. Melalui pihak Sertifikasi (*Certification Authority*) yang di dalam UU ITE disebut sebagai Penyelenggara Sertifikasi Elektronik (PSrE) seharusnya diberikan keterangan mengenai fungsi lainnya. Salah satunya terkait sertifikat untuk situs dagang milik Pelaku Usaha yang mana sertifikat tersebut dalam bentuk elektronik.

LSK mempunyai beberapa kategori penilaian untuk diakukan pemeriksaan terhadap Pelaku Usaha yang mendaftar. Salah satu hal krusial dalam kategori pemeriksaan tersebut adalah kategori terkait pengamanan terhadap pertukaran data yaitu dengan adanya Sertifikat Elektronik untuk identitas dan keamanan situs web

sekaligus sertifikat SSL. Hal ini dapat dilihat pada Penjelasan Pasal 68 ayat (1) PP PSTE 82/2012, pada kategori huruf b. Apabila sesuai dengan kriteria mereka maka SK dapat diterima oleh pelaku usaha, kemudian LSK menjaminnya dengan logo *trust mark*.

Dari keterangan diatas dapat disimpulkan bahwa PSrE yang berwenang menerbitkan Sertifikat Elektronik sedangkan LSK hanya sebagai tim penilai dan penjamin keandalan Pelaku Usaha namun tidak sampai berwenang atau mampu menerbitkan Sertifikat Elektronik untuk identitas dan keamanan situs web yaitu sertifikat SSL. Hal tersebut hanya menjadi salah satu kategori penilaian mereka.

Rancangan peraturan menteri (RPM) tentang LSK akan menjadi faktor pendorong pertumbuhan LSK lokal dan memberikan lahan bisnis baru bagi industri TI dalam negeri. Adapun selama ini, agar situs penyelenggara transaksi elektronik dapat dipercaya, mereka menggunakan LSK luar negeri, salah satunya *Verisign*. Kepala Proyek Indonesia *Incorporated* PT Telekomunikasi Indonesia Tbk (Telkom) sekaligus mantan koordinator sub tim LSK PP No.82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Saiful Hidayat bahwa saat ini di Indonesia belum ada LSK yang dikomersialisasi umum. Tujuannya agar para penyelenggara sistem dan transaksi elektronik beralih menggunakan LSK lokal.[18]

LSK lokal memiliki lebih banyak nilai lebih dibandingkan dengan LSK asing, salah satunya operasional di dalam negeri. LSK lokal mampu melakukan cek lokasi hingga bidang usaha penyelenggara sistem dan transaksi elektronik. Selain itu, regulasi tersebut nantinya dapat mendorong LSK asing membuka perusahaan di Indonesia untuk meningkatkan pelayanan ke konsumen. Contoh, Malaysia yang telah bekerja sama dengan *VeriSign* untuk membentuk *Multimedia Super Corridor (MSC) Trustgate* sebagai LSK.[19]

Konsep berikutnya juga bisa dengan hal ini, kalau LSK dicontohkan seperti *Verisign* maka seharusnya LSK bukan hanya sekedar menilai sang Pelaku Usaha namun juga diberikan

[18] Febrany D. A. Putri. *Lembaga Sertifikasi Keandalan: Rancangan Permen Akan Pacu LSK Lokal*. 2013. http://industri.bisnis.com/read/20130401/105/5967/lembaga-sertifikasi-keandalan-rancangan-permen-akan-pacu-lsk-lokal, hlm1. Diakses pada tanggal 19/7/2018.

[19] *Ibid*

keterangan pada aturan tertulisnya bahwa LSK juga dapat menerbitkan Sertifikat Elektronik berjenis Sertifikat Server Web bernama Sertifikat SSL, layaknya seperti yang dilakukan PSrE pula.

Konsep untuk Sertifikat Elektronik, bahwa secara umum pengertian mengenai Sertifikat Elektronik sudah benar hal ini sesuai dengan tampilan Sertifikat baik untuk kepentingan Tanda Tangan Elektronik saja atau lebih detail sebagai tanda Pelaku Usaha (Situs *Online*) yang bersertifikat.

Fungsi sertifikat elektronik itu sendiri mempunyai fungsi lain. Hal yang bisa diwakilkan oleh Sertifikat tersebut misalnya untuk menunjukkan kepemilikan Tanda Tangan Elektronik yang tersertifikasi milik subjek hukum dan fungsi lainnya yaitu sertifikat tersebut dapat mewakili subjek hukum yang menggunakan Sertifikat Server Web bernama Sertifikat SSL khususnya yang digunakan Pelaku Usaha di situs *online*nya atau aplikasi berbasis web. Walaupun saat ini penggunaan masih melibatkan jasa pihak asing dengan Sertifikat SSL yang dipunyai oleh pihak asing seperti dari *Digicert* dan *Comodo*. Hal-hal seperti ini tentunya juga perlu diakui secara hukum terutama dari segi fungsinya tadi. Jadi, dari segi aturan bukan hanya dimasukkan dari segi kategori penilaian oleh LSK. Namun, juga dapat dilihat dari berbagai fungsi dari Sertifikat Elektronik.

Hal **kedua**, yaitu mengenai wajib atau tidaknya penggunaan Sertifikat Elektronik untuk kepentingan situs web (Sertifikat SSL) ini dalam program Sertifikasi untuk Pelaku Usaha di Indonesia. Penggunaan Sertifikat Elektronik untuk situs web (sertifikat SSL) ini menjadi salah satu kategori pemeriksaan untuk menjamin keandalan Sistem Elektronik milik Pelaku Usaha tersebut agar bisa mendapatkan Sertifikat Keandalan (SK) dari Lembaga Sertifikasi Keandalan (LSK). Dari segi aturan, pada pasal 10 ayat (1) UU ITE 11/2008 hanya menyebutkan bahwa "Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan". Dari isi pasal tersebut masih belum ada keterangan tentang kewajiban sertifikasi.

Kemudian pada PP PSTE 82/2012 Pasal 42 ayat (1) juga tidak ditemukan tentang keterangan kewajiban penggunaan Sertifikat Elektronik untuk situs web (sertifikat SSL) ini menjadi

salah satu kategori pemeriksaan untuk sertifikasi untuk menjamin keandalan Sistem Elektronik milik Pelaku Usaha tersebut agar bisa mendapatkan Sertifikat Keandalan (SK) dari Lembaga Sertifikasi Keandalan (LSK). PP PSTE 82/2012 Pasal 42 ayat (1) bahwa "Penyelenggaraan Transaksi Elektronik dalam lingkup privat dapat menggunakan Sertifikat Keandalan dan/atau Sertifikat Elektronik". Jenis hubungan transaksi elektronik misalnya antar pelaku usaha dengan konsumen (BtoC) yang termasuk ke dalam Penyelenggaraan Transaksi Elektronik dalam lingkup privat (Pasal 40 ayat (3) PP PSTE 82/2012).

Menyambung hal diatas, selaras dengan aturan tersebut dilansir dari artikel pada halaman situs web Kementerian Komunikasi dan Informatika (Kominfo) bahwa mengenai syarat sertifikasi (Sertifikasi Keandalan) untuk usaha rintisan (*startup*) Perdagangan berbasis Elektronik (*E-Commerce*) tidak diwajibkan bagi pelaku usaha perdagangan elektronik. Hal ini disertai dengan alasan bahwa pemerintah tidak punya kapasitas untuk mengatur sertifikasi, pemerintah ingin membuka kesempatan bagi startup. Pemerintah tidak ingin syarat sertifikasi mempersulit masyarakat untuk memulai startup.[20]

Seperti diketahui bahwa salah satu kategori sertifikasi keandalan adalah mempunyai sertifikat elektronik berjenis sertifikat server bernama sertifikat SSL. Dengan tidak diwajibkannya sertifikasi berarti menandakan bahwa kategori sertifikat SSL pun juga tidak diwajibkan penggunaanya. Apabila ditelaah lebih dalam, pada dasarnya hal ini juga menjadi tanggung jawab si pelaku usaha yang berniat ingin mempunyai situs usaha serta aplikasi perdagangan secara *online* di dunia internet karena ini untuk keamanan sang pelaku usaha sekaligus bermanfaat untuk calon pembeli.

Bahwa dengan didahului kenyataan bahwa pihak Sertifikasi belum terbentuk di Indonesian serta diiringi dengan keputusan bahwa proses sertifikasi untuk pelaku usaha yang tidak mengarah ke wajib maka otomatis penggunaan Sertifikat SSL juga bukan hal yang wajib bagi pelaku usaha yang memiliki situs web untuk

[20] Indah Rahmayani. *Syarat Sertifikasi Startup e-Commerce Dihapus*. 2015. https://kominfo.go.id/content/detail/6119/syarat-sertifikasi-startup-e-commerce dihapus/0/sorotan_media. Diakses pada tanggal 22/10/2018.

usaha perdagangan *online* dengan kata lain yaitu bersifat opsional.

Hal **ketiga** yaitu peran Pemerintah misalnya membentuk suatu komisi khusus yang menangani dalam hal membuat daftar resmi 5 atau 10 besar kumpulan daftar peringkat situs dagang *online* milik pelaku usaha yang diketahui sistem keamanannya terbaik disertai dengan hasil presentase kepuasaan konsumen, hal ini dapat diukur dari data dilapangan yang dikumpulkan sampelnya oleh Pemerintah langsung. Hal-hal ini diharap dapat menstimulasi pelaku usaha untuk bersaing agar situs usahanya bisa masuk daftar tersebut. Dengan bersaing meningkatkan kualitas keamanan sistem elektronik mereka serta pelayanan mereka termasuk penggunaan sertifikat SSL. Konsumen pun akan kurang yakin memilih suatu situs belanja apabila situs usaha *online* Pelaku Usaha tersebut tidak dapat masuk dalam daftar tersebut. Dengan didorong oleh faktor-faktor tersebut diharap kemudian dapat memicu pertumbuhan Otoritas Sertifikasi/CA baik itu milik Pemerintah atau pihak swasta dalam negeri, agar Pelaku Usaha diwajibkan menggunakan layanan Sertifikat SSL dari dalam negeri sendiri.

Perlu diperhatikan, mempersiapkan program akreditasi dari dalam negeri (internal), untuk menguji sistem keamanan dan infrastruktur Otoritas Sertifikasi/CA tersebut, karena tentunya tidak ada sistem yang 100% aman. Hal ini dimaksudkan untuk persiapan apabila pertumbuhan Otoritas Sertifikasi/CA sudah terlihat signifikan. Hal ini juga ditujukan agar CA komersil yang nanti hadir mereka akan berlomba-lomba untuk meningkatkan tingkat keamanannya dan pemerintah dapat mengumumkan atau merangking CA yang paling banyak dipercaya atau dipilih masyarakat.

Dalam teori utilitas dari Jeremy Bentham, yang berpendapat bahwa hukum itu bertujuan memberikan manfaat bagi manusia. Pada teori ini menetapkan bahwa tujuan hukum adalah untuk memberikan manfaat sebanyak-banyaknya.[21] Dalam bukunya "*Introduction to the morals and leg-islation*", Jeremy Bentham mengatakan bahwa hukum bertujuan semata-mata apa yang berfaedah bagi orang. Kepastian melalui hukum bagi

[21] Zulkarnaen dan Beni Ahmad Saebeni. 2012. *Hukum Konstitusi*. Bandung: Pustaka Setia. hlm 26

perorangan merupakan tujuan utama dari pada hukum.[22]

Jadi, kegunaan sertifikat SSL lewat layanan CA publik milik negara sendiri maka nantinya bukan hanya berguna untuk para pelaku usaha saja namun juga bank-bank milik negara Indonesia. Karena kalau untuk pelaku usaha gunanya untuk situs web. Ada baiknya data-data pribadi konsumen sekaligus perbankan nasional berada di tangan negara sendiri tidak dipihak asing kecuali bank tersebut memang milik pihak asing. Ditambah lagi sekarang terdapat Gerakan Nasional 1000 *Start Up* (usaha rintisan) Digital. Dengan beresnya mengenai sertifikasi di Indonesia, semoga membawa manfaat kepada para pelaku usaha tersebut.

KESIMPULAN

A. 1. Para pihak dalam transaksi perdagangan elektronik (lingkup privat) hubungan pelaku usaha dengan konsumen/BtoC, terdiri dari Penjual dan Pembeli, serta pihak Bank, Otoritas Sertifikasi (*Certification Authority*), *Acquier, Issuer*, Penyedia Jasa Internet, Jasa Pengiriman dan Pemerintah.

2. Penggunaan sertifikasi elektronik dalam sistem perdagangan elektronik yaitu melalui layanan dari Otoritas Sertifikasi yang menerbitkan Sertifikat Elektronik berjenis Sertifikat Server bernama Sertifikat *Secure Sockets Layer* (SSL) bermanfaat untuk pelaku usaha yang mempunyai situs web dagang di internet untuk mengotentikasi identitas situs web serta mengamankan ruang saluran komunikasi yang terjalin dalam situs.

3. Hubungan perikatan para pihak dalam transaksi perdagangan elektronik dengan menggunakan sertifikasi elektronik yaitu atas dasar jual beli didunia internet maka Penjual mempunyai kewajiban untuk memberikan suatu dasar perlindungan keamanan terhadap Pembeli yaitu dalam proses bertransaksi perdagangan di dunia internet dan memenuhi hak konsumen untuk mendapatkan keamanan dalam berbelanja karena itu Penjual menggunakan jasa dari Otoritas Sertifikasi untuk penerbitan Sertifikat Elektronik berjenis Sertifikat Server bernama Sertifikat SSL.

B. 1. Peraturan hukum di Indonesia yang mengatur Sertifikasi Elektronik, secara umum untuk isi tampilan Sertifikat bisa dijelaskan dengan UU ITE dan PP PSTE. Namun, untuk

[22] R Soeroso. 2011. *Pengantar Ilmu Hukum*. Jakarta: Sinar Grafika. hlm 58-59

kewenangan PSrE dan fungsi Sertifikat Elektronik yang mengarah ke Sertifikat Server berjenis Sertifikat SSL dirasa belum detail. Sertifikat SSL merupakan salah satu kategori penilaian dari LSK kepada Pelaku Usaha.

2. Bentuk sistem sertifikasi elektronik di beberapa negara yaitu Singapura mempunyai Otoritas Sertifikasi bernama *Netrust* yang mampu menerbitkan Sertifikat Elektronik untuk Server (sertifikat SSL) dan Pemerintah AS mengizinkan sektor swasta untuk menerapkan kebijakan privasi mereka sendiri. Salah satu cara yang diadopsi oleh pedagang di Internet yaitu menerapkan layanan otentikasi Sertifikat Elektronik untuk Server (sertifikat SSL) melalui CA seperti *Verisign*.

3. Perspektif penggunaan sertifikasi elektronik dalam perdagangan di Indonesia mengenai fungsi Otoritas Sertifikasi dan fungsi lain dari Sertifikat Elektronik sebagai tanda bahwa situs pelaku usaha sudah bersertifikat. Keikutsertaan peran Pemerintah dengan mewajibkan syarat Sertifikasi Elektronik untuk Pelaku Usaha (Penjual) dan mewajibkan Pelaku Usaha dalam negeri serta Pelaku Usaha dari luar Indonesia yang membuka cabang bisnisnya di Indonesia diwajibkan menggunakan Sertifikat Elektronik (Sertifikat SSL) dari dalam negeri (Indonesia).

DAFTAR PUSTAKA

- **Buku-Buku**

Badrulzaman, Mariam Darus, dkk. 2001. *Kompilasi Hukum Perikatan*. Bandung: PT. Citra Aditya Bakti.

Barkatullah, Abdul Halim. 2017. *Hukum Transaksi Elektronik Sebagai Panduan dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia*,
Bandung: Nusa Media.

Mertokusumo, Sudikno. 2003. *Mengenal Hukum Suatu Pengantar*. Yogyakarta: Liberty.

Pratama, I Putu Agus Eka. 2014. *Komputer dan Masyarakat*. Bandung: Informatika.

Sarwono, Jonathan dan K. Prihartono AH. 2012. *Perdagangan Online : Cara Bisnis Di Internet*. Jakarta: PT Elex Media Komputindo.

Soeroso, R. 2011. *Pengantar Ilmu Hukum*. Jakarta: Sinar Grafika.

Sukandar, Dadang. 2017. *Panduan Membuat Kontrak Bisnis*. Jakarta: Visimedia.

Widijawan, Dhanang. 2018. *Dasar-Dasar Hukum Kontrak Bisnis Transaksi & Sistem Elektronik (UU ITE Perubahan No. 19/2016)*. Bandung: Keni Media.

Zulkarnaen dan Beni Ahmad Saebeni. 2012. *Hukum Konstitusi*. Bandung: Pustaka Setia.

- **Jurnal**

  Barkatullah, Abdul Halim dan Djumadi. *Does self-regulation provide legal protection and security to e-commerce consumers?*. 2018. Artikel dalam "Jurnal Elsevier". May, hlm. 96.

- **Artikel, Makalah dan Karangan dalam Buku dan Internet**

  Direktorat Jenderal Aplikasi Informatika. *Sivion-Solusi Identitas Digital Terpercaya*. 2016. https://aptika.kominfo.go.id/index.php/artikel/134-sivion-solusi-identitas-digital-terpercaya. Diakses pada tanggal 1/7/2018.

  IndonesiaGo Digital. *Fungsi Serta Pentingnya Sertifikasi SSL (HTTPS) Bagi Website Anda* . 2017. https://indonesiago.digital/sertifikasi-ssl-https-bisnis-anda/. Diakses pada tanggal 5/7/2018.

  Netrust Pte Ltd. https://www.netrust.net/about/. Diakses pada tanggal 26/7/2018.

  Putri, Febrany D. A. *Lembaga Sertifikasi Keandalan: Rancangan Permen Akan Pacu LSK Lokal*. 2013. http://industri.bisnis.com/read/20130401/105/5967/lembaga-sertifikasi-keandalan-rancangan-permen-akan-pacu-lsk-lokal. Diakses pada tanggal 19/7/2018.

  Rahmayani, Indah. *Syarat Sertifikasi Startup e-Commerce Dihapus*. 2015. https://kominfo.go.id/content/detail/6119/syarat-sertifikasi-startup-e-commerce dihapus/0/sorotan_media. Diakses pada tanggal 22/10/2018.

  VeriSign, Inc. *Semua yang Perlu Anda Ketahui Tentang Sertifikat SSL*. https://www.verisign.com/in_ID/website-presence/website-optimization/ssl-certificates/index.xhtml. Diakses pada tanggal 1/7/2018.

  Widiartanto, Yoga Hastyadi. *Bukalapak dan Tokopedia Jelaskan Aplikasinya yang Lacak Data Pengguna*. 2016. https://tekno.kompas.com/read/2016/11/02/13020077/bukalapak.dan.tokopedia.jelaskan.aplikasinya.yang.lacak.data.pengguna.. Diakses pada tanggal 1/7/2018.

- **Kamus-kamus**

  Marhiyanto, Bambang. *Kamus Lengkap Bahasa Indonesia*. Surabaya: Media Centre

- **Peraturan Perundang-undangan**

  Kitab Undang-Undang Hukum Perdata (Staatsblad 1847 Nomor 23)

  Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik. Republik Indonesia. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

  Republik Indonesia. Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan.

  Republik Indonesia. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

- **Berita dan Tajuk Rencana dalam Surat Kabar dan Internet**

  www.kemenkeu.go.id. "*Nilai Perdagangan E-Commerce di Indonesia Masih Rendah*". Diakses pada tanggal 1 April 2018