

**PEMANFAATAN TANDA TANGAN DIGITAL TERSERTIFIKASI DI
ERA PANDEMI**

*(UTILIZATION OF CERTIFIED DIGITAL SIGNATURES IN THE
PANDEMIC ERA)*

Rizki Dermawan

Fakultas Syariah Institut Agama Islam Negeri (IAIN) Kediri

Korespondensi Penulis : rizkidermawan@iainkediri.ac.id

Citation Structure Recommendation :

Dermawan, Rizki. *Pemanfaatan Tanda Tangan Digital Tersertifikasi di Era Pandemi*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.2. No.8 (Agustus 2021).

ABSTRAK

Di era digital, beberapa hal menjadi mudah didapatkan. Misalnya apabila bertransaksi dengan *E-Commerce* maka barang yang dipesan melalui ponsel langsung datang ke konsumen. Begitu pun proses penandatanganan dokumen yang beralih ke digital. Untuk melindungi kegiatan transaksi digital, maka pemerintah telah mengatur pada UU ITE dan turunan lainnya. Pengetahuan mengenai tanda tangan digital sangat diperlukan karena memiliki konsekuensi dan pertanggung jawaban. Tanda tangan digital yang telah tersertifikasi sudah mendapatkan sertifikat elektronik. Masih ada kendala pada penerapan tanda tangan digital dan berharap pemahaman masyarakat mengenai tanda tangan digital semakin baik sehingga mendorong mempermudah kehidupan sehari-hari.

Kata Kunci: *E-Commerce*, Sertifikasi, Tanda Tangan Digital

ABSTRACT

In the digital era, several things have become easy to find. For example, transacting with e-commerce so goods ordered via cell phones come directly to consumers. Likewise, the document signing process has switched to digital. To protect digital transaction activities, the government has regulated the Information and Electronic Transactions (a.k.a ITE) law and other derivatives. Knowledge of digital signatures is needed because it has consequences and responsibilities. Digital signatures that have been certified have received an electronic certificate. There are still obstacles in the application of digital signatures and hope that people's understanding of digital signatures will improve so as to make everyday life easier.

Keywords: *E-Commerce*, Certification, Digital Signature

A. PENDAHULUAN

Di era revolusi digital ini, beberapa hal menjadi mudah untuk didapatkan. Misalnya konsumen yang bertransaksi melalui perdagangan elektronik atau *E-Commerce*, maka barang yang dipesan dan dibayar melalui ponsel pintar akan langsung datang ke rumah konsumen. Tidak terkecuali dengan dunia pemerintahan, tren digital ini juga ikut berkembang. Banyak instansi yang berlomba-lomba memberikan pelayanan publik kepada masyarakat dengan memanfaatkan kecanggihan teknologi informasi dan komunikasi.¹

Kemudahan dalam bertransaksi elektronik ini dimanfaatkan sebagian orang atau pengusaha untuk menjalankan kegiatan usahanya. Terlebih di kala pandemi Covid-19 yang melanda seluruh negara, membuat terbatasnya ruang gerak semua orang untuk berkegiatan. Transformasi transaksi elektronik dari awal mulanya bertransaksi secara langsung berubah menjadi transaksi dalam bentuk elektronik guna meminimalisasi penularan Covid-19. Di Indonesia saat ini mengalami beberapa transformasi untuk mengembangkan teknologi digital, salah satu bentuk yang terjadi adalah mulai dilakukannya penerapan Tanda Tangan Digital.

Untuk melindungi masyarakat saat melakukan transaksi elektronik ataupun khususnya membuat Tanda Tangan Digital, maka pemerintah telah mengeluarkan berbagai regulasi seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Diikuti dengan aturan turunan meliputi Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).

Pengetahuan dan pemahaman mengenai Tanda Tangan Digital sangat diperlukan karena memiliki konsekuensi dan pertanggung jawaban. Guna mewujudkan hal tersebut, perlu adanya sarana dan prasarana pendukung terkait pelaksanaan Tanda Tangan Digital ini. PSrE hadir sebagai pelopor nasional penyelenggara sertifikat elektronik yang dikelola oleh Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika Republik Indonesia.

¹ Ita Wijayanti, *Pemerintahan Berbasis Elektronik dalam Pelayanan Publik*, diakses dari <https://ombudsman.go.id/artikel/r/artikel--pemerintahan-berbasis-elektronik-dalam-pelayanan-publik>, diakses pada 20 April 2021.

Adapun PSrE merupakan kepanjangan dari Penyelenggara Sertifikat Elektronik yang bertujuan untuk menyediakan jasa sertifikat dan tanda tangan digital yang efisien, aman, dan praktis bagi ekosistem digital di Indonesia, terutama untuk ekosistem dalam industri keuangan dan transaksi *E-Commerce*.²

Tanda Tangan Digital dan Tanda Tangan Elektronik merupakan dua hal yang berbeda. Perbedaan ini terlihat dengan jelas dari segi keamanannya, keasliannya, keabsahannya dan kerahasiaan data pemilik tanda tangan. Namun pada kenyataannya, masih banyak orang yang salah dalam mendefinisikan dan mengartikan dua hal tersebut.³ Pasal 1 angka 12 UU ITE menjelaskan 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.

Tanda Tangan Elektronik merujuk kepada data dalam bentuk elektroniknya, yang dilekatkan kepada sebuah dokumen elektronik. Data tersebut merupakan informasi elektronik dari penandatanganan dan bentuknya tidak terbatas hanya pada tanda tangan basah (tulisan tangan) yang dibuat ke dalam bentuk elektronik. Sedangkan Tanda Tangan Digital merupakan sebuah mekanisme kriptografi yang sering diimplementasikan ke dalam Tanda Tangan Elektronik. Informasi yang dilekatkan dengan menggunakan Tanda Tangan Digital tidak hanya sekedar data atau tanda tangan dalam bentuk elektroniknya, tetapi juga sebuah data terenkripsi dan sertifikat digital dari pemilik Tanda Tangan Digital.⁴

Tanda Tangan Digital bukan tanda tangan yang dibubuhkan di atas kertas sebagaimana lazimnya suatu tanda tangan. Tanda Tangan Digital diperoleh dengan terlebih dahulu menciptakan yang disebut *Message Digest* atau *Hast*, yaitu *Mathematical Summary* dokumen yang dikirimkan melalui *Cyberspace*.⁵

² Kementerian Komunikasi dan Informatika Republik Indonesia, *Apa Itu Penyelenggara Sertifikasi Elektronik*, diakses dari <https://tte.kominfo.go.id/apaitu#sebuah-perkenalan>, diakses pada 20 April 2021.

³ Dinas Komunikasi Informatika dan Statistik Kabupaten Ponorogo, *Tanda Tangan Elektronik vs Tanda Tangan Digital*, diakses dari <https://kominfo.ponorogo.go.id/tanda-tangan-elektronik-vs-tanda-tangan-digital/>, diakses pada 19 April 2021.

⁴ Privy Indonesia, *Tanda Tangan Elektronik vs Tanda Tangan Digital*, diakses dari <https://blog.privyy.id/tanda-tangan-elektronik-vs-tanda-tangan-digital/>, diakses pada 19 April 2021.

⁵ Soemarno Partodihardjo, *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*, Penerbit Gramedia Pustaka Utama, Jakarta, 2009, p.20.

Hal ini berbeda dari tanda tangan biasa yang berfungsi sebagai pengakuan dan penerimaan atas isi pesan atau dokumen. Tanda Tangan Digital adalah suatu *item* data yang berhubungan dengan sebuah pengkodean pesan digital guna memberi kepastian tentang keaslian data dan memastikan bahwa data tidak termodifikasi

Pasal 60 ayat (2) PP PSTE menyebutkan Tanda Tangan Elektronik ada yang tersertifikasi dan tidak tersertifikasi. Jika tidak tersertifikasi, maka aspek keamanannya tidak bisa dipenuhi dan mudah dipalsukan. Sedangkan Tanda Tangan Elektronik yang telah tersertifikasi sudah ditambahkan dengan penguatan sertifikat elektronik. Bila terjadi perubahan atau modifikasi dapat dengan mudah diketahui oleh sistem. Meski penggunaan Tanda Tangan Digital terus meningkat, ternyata masih terdapat kendala dalam penerapan dari Tanda Tangan Digital ini. Masih terdapat pula salah kaprah di masyarakat mengenai pemahaman tentang Tanda Tangan Digital. Ada anggapan bahwa Tanda Tangan Digital merupakan tanda tangan basah di atas kertas yang dipindai ke dalam file komputer.

Lebih lanjut lagi, terdapat persoalan lain yaitu kerahasiaan Tanda Tangan Digital. Salah satu risiko yang masih dikhawatirkan masyarakat yaitu pencurian data pribadi pengguna. Sebab, pembubuhan tanda tangan melalui pihak ketiga atau penyelenggara sistem elektronik dikhawatirkan dapat disalahgunakan pihak yang tidak bertanggung jawab. Pasal 52 ayat (3) PSTE menjelaskan dalam hal terjadi penyalahgunaan Tanda Tangan Elektronik oleh pihak lain yang tidak berhak, tanggung jawab pembuktian penyalahgunaan Tanda Tangan Elektronik dibebankan kepada Penyelenggara Sistem Elektronik.

Penulisan ini menggunakan tipe penelitian normatif, yang tergolong sebagai penelitian hukum untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum yang relevan dan melakukan telaah mengenai konsep-konsep hukum, pendapat para ahli hukum untuk meningkatkan daya interpretasi guna menjawab isu hukum yang dihadapi.⁶ Penelitian ini akan menempatkan peraturan atau norma-norma positif di dalam sistem perundang-undangan sebagai sumber utama untuk membahas tentang pertanggungjawaban penyelenggara sertifikasi elektronik pada Tanda Tangan Digital dan perlindungan hukum bagi pengguna Tanda Tangan Digital tersertifikasi.

⁶ Peter Mahmud Marzuki, *Penelitian Hukum*, Penerbit Prenadamedia Group, Jakarta, 2016, p.35.

Pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.⁷ Pemahaman akan pandangan-pandangan dan doktrin-doktrin tersebut merupakan sandaran bagi peneliti untuk membangun argumentasi hukum dalam memecahkan isu hukum yang diteliti. Pendekatan Undang-undang (*Statute Approach*) dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkutan paut dengan isu hukum yang sedang ditangani.⁸ Hasil dari telaah tersebut adalah suatu argumen untuk dapat memecahkan isu hukum yang akan diteliti.

Mencermati uraian diatas terkait kerahasiaan Tanda Tangan Digital, maka salah satu risiko yang dikhawatirkan masyarakat yaitu pencurian data pribadi pengguna yang dapat disalahgunakan pihak yang tidak bertanggung jawab. Penelitian ini dilakukan untuk menjawab rumusan permasalahan atau isu hukum tentang **“Apa Bentuk Pertanggungjawaban Penyelenggara Sertifikasi Elektronik pada Tanda Tangan Digital?”** dan **“Bagaimana Perlindungan Hukum Bagi Pengguna Tanda Tangan Digital Tersertifikasi?”**.

B. PEMBAHASAN

1. Pertanggungjawaban Penyelenggara Sertifikasi Elektronik pada Tanda Tangan Digital

Penggunaan transaksi elektronik untuk kegiatan usaha melalui perdagangan elektronik atau *E-Commerce* memberikan kemudahan bagi pelaku usaha dan juga konsumen untuk berinteraksi jual beli. Transaksi perdagangan *E-Commerce* dapat muncul saat terjadinya kesepakatan perjanjian jual beli antara produsen dan konsumen yang berdasarkan pada hukum.⁹ Tanpa bertemu sekali pun, kedua pihak yang bertransaksi harus melakukan kegiatan transaksi perdagangan sesuai dengan kesepakatan dan aturan perundang-undangan.

⁷ Peter Mahmud Marzuki, *Penelitian Hukum*, Penerbit Prenadamedia Group, Jakarta, 2016, p.135.

⁸ Peter Mahmud Marzuki, *Ibid.*, p.158.

⁹ Achmad Busro, *Hukum Perikatan Berdasarkan Buku III KUH Perdata*, Penerbit Pohon Cahaya, Yogyakarta, 2011, p.8.

Penggunaan internet dipilih oleh kebanyakan pelaku usaha dan konsumen dikarenakan kemudahan-kemudahan yang disediakan oleh jaringan internet, seperti mempermudah pekerjaan dalam mendapatkan informasi dengan cepat. Pada dasarnya, manfaat dari mengakses internet adalah adanya kemudahan dalam pencarian informasi, baik terkait kehidupan pribadi, maupun terkait informasi profesional pekerjaan. Terdapat tiga tahapan dalam pelaksanaan transaksi pada *E-Commerce* yaitu sebagai berikut¹⁰:

- a. Tahap pra-kontraktual dalam pelaksanaan transaksi jual beli *E-Commerce*.
- b. Tahap kontraktual dalam pelaksanaan transaksi jual beli *E-Commerce*.
- c. Tahap post kontraktual dalam pelaksanaan transaksi jual beli *E-Commerce*.

Pasal 1 angka 10 UU ITE menjelaskan, Penyelenggara Sertifikat Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik. PSrE induk adalah penyelenggara sertifikat elektronik atau *Certification Authority* yang dijalankan oleh pemerintah Indonesia di bawah Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika Indonesia yang menerbitkan Sertifikat Elektronik bagi Penyelenggara Sertifikasi Elektronik berinduk. Sedangkan PSrE berinduk adalah penyelenggara sertifikat elektronik atau *Certification Authority* yang telah diakui oleh PSrE induk untuk menjalankan jasa sertifikat digital yang dilakukan baik oleh perseorangan Warga Negara Indonesia atau Warga Negara Asing, organisasi maupun badan usaha penyelenggara Sertifikat Elektronik yang berdomisili di Indonesia maupun yang memiliki kepemilikan modal asing.

Pada transaksi teknologi finansial yang dilakukan melalui internet, tanda tangan yang digunakan juga berupa tanda tangan dalam bentuk data elektronik, yang kemudian dikenal sebagai tanda tangan elektronik. Yang dimaksud dengan *Digital Signature* atau *Electronic Signature* bukanlah *Digitized Image of Handwritten* atau bukan tanda tangan atau gambar. Akan tetapi adalah dengan cara membuat suatu *Hash* atau *Message Digest* terlebih dahulu, berupa dokumen *Mathematical Summary* yang akan dikirim melalui *Cyber Space*.¹¹

¹⁰ Thamaroni Usman, *Keabsahan Tanda Tangan Elektronik Pada Perjanjian Jual Beli Barang dari Perspektif Hukum Perdata*, IPLR, Vol.1, Issue 2 (Juli-Desember 2020), p.89.

¹¹ Yahya Harahap, *Hukum Acara Perdata: Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan*, Penerbit Sinar Grafika, Jakarta, 2015, p.563.

Penyelenggaraan Sertifikasi Elektronik diatur pada Pasal 13 dan Pasal 14 UU ITE sebagai berikut:

Pasal 13

- (1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.
- (2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.
- (3) Penyelenggara Sertifikasi Elektronik terdiri atas:
 - a. Penyelenggara Sertifikasi Elektronik Indonesia; dan
 - b. Penyelenggara Sertifikasi Elektronik asing.
- (4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
- (5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
- (6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud dalam Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

- a. Metode yang digunakan untuk mengidentifikasi Penanda Tangan;
- b. Hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan
- c. Hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

Setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk membuat sebuah tanda tangan digital. Penyelenggara sertifikasi elektronik ini harus berbadan hukum dan terdaftar di Indonesia. Terdapat tujuh perusahaan yang sudah mendapatkan status pengakuan sebagai Penyelenggara Sertifikasi Elektronik yaitu: PT Privy Identitas Digital, PT. Solusi Net Internusa, Perusahaan Umum Percetakan Uang Republik Indonesia, PT. Indonesia Digital Identity (VIDA), PT. Djelas Tandatangan Bersama, Badan Pengkajian dan Penerapan Teknologi dan Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara.¹²

Kewajiban Penyelenggara Sertifikasi Elektronik diatur lebih lanjut pada Peraturan Menteri Kominfo Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik (Permenkominfo PSE). Dijelaskan pada Pasal 21 bahwa Penyelenggara Sertifikasi Elektronik wajib melaksanakan hal sebagai berikut:

¹² Kementerian Komunikasi dan Informatika Republik Indonesia, *Status Pengakuan Penyelenggara Sertifikasi Elektronik*, diakses dari <https://tte.kominfo.go.id/listPSrE/>, diakses pada 19 April 2021.

- a. Menyelenggarakan proses administrasi bagi pemohon Sertifikat Elektronik;
- b. Memverifikasi kebenaran identitas pemohon Sertifikat Elektronik;
- c. Memastikan masa berlaku Sertifikat Elektronik;
- d. Melakukan perpanjangan masa berlaku Sertifikat Elektronik terhadap Pemilik Sertifikat Elektronik yang mengajukan perpanjangan masa berlaku;
- e. Membuat basis data Sertifikat Elektronik yang aktif dan yang dibekukan serta memelihara dokumen arsip secara sistematis dan dapat dipertanggungjawabkan baik dalam bentuk tertulis (*Paper Based*) dan elektronik (*Electronic Based*);
- f. Menempatkan dan memublikasikan Sertifikat Elektronik ke dalam sistem penyimpanan (*Repository*);
- g. Menjaga kerahasiaan identitas Pemilik Sertifikat Elektronik dari pihak yang tidak berkepentingan;
- h. Memberitahukan Kebijakan Sertifikat Elektronik (*Certificate Policy*) dan/atau Pernyataan Penyelenggaraan Sertifikasi Elektronik (*Certification Practice Statement*) Penyelenggaraan Sertifikasi Elektroniknya kepada calon Pemilik Sertifikat Elektronik dan Pemilik Sertifikat Elektronik yang diterbitkannya; dan
- i. Memberikan laporan operasional periodik dan sewaktu-waktu kepada Menteri mengenai aktivitas Penyelenggaraan Sertifikasi Elektronik yang dilakukannya.

Seperti dijelaskan diatas bahwa penyelenggara sertifikasi elektronik memiliki kewajiban, salah satunya terdapat pada huruf g yaitu menjaga kerahasiaan identitas pemilik sertifikat elektronik dari pihak yang tidak memiliki kepentingan. Aturan Pasal 21 huruf g Permenkominfo PSE jika tidak dijalankan dengan baik oleh penyelenggara sertifikasi maka akan ada sanksi seperti tertuang pada Pasal 43 ayat (1) Permenkominfo PSE yang menjelaskan: Menteri memberikan sanksi administratif pada Penyelenggara Sertifikasi Elektronik yang melakukan pelanggaran ketentuan sebagaimana dimaksud dalam Pasal 4 ayat (3), Pasal 17 ayat (1), Pasal 17 ayat (2), Pasal 21, Pasal 22, Pasal 34 ayat (1), dan Pasal 34 ayat (2). Sanksi administratif sebagaimana dimaksud pada Pasal 43 ayat (1) Permenkominfo PSE yang meliputi:

- a. Teguran tertulis;
- b. Penghentian sementara pendaftaran Pemilik Sertifikat Elektronik; dan/atau
- c. Dikeluarkan dari daftar.

Pasal 57 ayat (1) PP PSTE menjelaskan bahwa Penyelenggara Sertifikasi Elektronik Indonesia menyediakan layanan yang tersertifikasi salah satunya adalah Tanda Tangan Elektronik. Tanda tangan pada umumnya mempunyai arti yang lebih luas yaitu segala suatu kode atau tanda yang kegunaannya sebagai alat legalisasi dokumen yang ditandatangani.¹³ Sedangkan tanda tangan elektronik mempunyai arti yang lebih sempit yaitu penerapan sekumpulan teknik-teknik komputer terhadap suatu informasi yang berguna untuk menjaga keamanan dokumen.¹⁴ Klasifikasi Tanda Tangan Elektronik sebagai berikut¹⁵:

- a. Tanda Tangan Elektronik (Biasa). Tanda tangan elektronik biasa, sesuai dengan pengertian mengenai tanda tangan elektronik di atas adalah tanda tangan yang ditujukan merujuk kepada si penanda tangan, yang dilakukan dengan media elektronik. Contoh paling mudah adalah suatu tanda tangan konvensional (tertulis) yang kemudian di-*scan*. Kemudian hasil *scan* tersebut akan menjadi suatu informasi elektronik, biasanya berupa suatu *file* gambar, ditempelkan (*paste*) pada suatu dokumen elektronik. Hal tersebut sudah termasuk dalam ruang lingkup tanda tangan elektronik (biasa).
- b. Tanda Tangan Elektronik yang Aman (*Secure* atau *Reliable*). Tanda tangan elektronik yang aman atau *Electronic Signature*, merupakan suatu tanda tangan elektronik yang harus memenuhi persyaratan-persyaratan tertentu, sehingga dalam konteks kesamaannya dapat dipersamakan dengan tanda tangan konvensional. Tanda tangan elektronik yang aman ini diperuntukkan untuk menampung semua jenis kemajuan teknologi yang mungkin berkembang dalam bidang keamanan terhadap informasi elektronik yang aman ditujukan untuk tidak hanya dapat merujuk kepada si penanda tangan, tetapi juga untuk menjaga keutuhan dan keamanan daripada suatu informasi elektronik yang dilekatkan. Tanda tangan digital termasuk di dalam kategori tanda tangan elektronik yang aman.

¹³ Abdul Kadir, *Hukum Perdata Indonesia*, Penerbit Citra Aditya Bakti, Bandung, 2000, p.38.

¹⁴ Reza Raditio, *Aspek Hukum Transaksi Elektronik: Perikatan, Pembuktian dan Penyelesaian Sengketa*, Penerbit Cipta Bakti, Yogyakarta, 2014, p.29.

¹⁵ Joan Venzka Tahapary, *Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti yang Sah Ditinjau Dalam Hukum Acara Perdata*, Tesis, Fakultas Hukum Universitas Indonesia, Depok, 2011, p.21.

Pemanfaatan Tanda Tangan Elektronik dapat mendorong peningkatan efektivitas dan efisiensi berbagai layanan sistem elektronik. Pemanfaatan Tanda Tangan Elektronik tetap dapat menyediakan aspek fleksibilitas keamanan informasi selain memberikan keuntungan secara ekonomi.¹⁶ Pasal 11 ayat (1) UU ITE menjelaskan bahwasanya Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

- a. Data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
- b. Data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
- c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
- d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
- e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatanganannya; dan
- f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Tanda Tangan Digital yang sesuai dengan ketentuan yang ditetapkan dan memperoleh sertifikat dari penyelenggara sertifikasi maka memiliki kekuatan hukum dan akibat hukumnya. Penyelenggara sertifikasi elektronik dalam menyimpan data pembuatan Tanda Tangan Digital wajib sesuai dengan ketentuan Pasal 63 ayat (3) PP PSTE dan Pasal 64 ayat (1) PP PSTE. Selanjutnya jika kewajiban tersebut tidak dilaksanakan oleh penyelenggara sertifikasi elektronik, maka akan dikenakan sanksi administratif seperti dijelaskan pada Pasal 100 PP PSTE mengenai sanksi berupa:

- a. Teguran tertulis;
- b. Denda administratif;
- c. Penghentian sementara;
- d. Pemutusan akses; dan/atau
- e. Dikeluarkan dari daftar.

Pasal 63 ayat (3) PP PSTE menjelaskan dalam hal Penyelenggara Sertifikasi Elektronik menyimpan Data Pembuatan Tanda Tangan Elektronik, Penyelenggara Sertifikasi Elektronik wajib:

¹⁶ BSSN, *Tanda Tangan Elektronik Si Mata Pena “The New Normal” Semangat Wujudkan Transformasi Digital Pemerintah*, diakses dari <https://bssn.go.id/tanda-tangan-elektronik-si-mata-pena-the-new-normal-semangat-wujudkan-transformasi-digital-pemerintah/>, pada 20 April 2021.

- a. Memastikan penggunaan Data Pembuatan Tanda Tangan Elektronik hanya berada dalam kuasa Penanda Tangan;
- b. Menggunakan Perangkat Pembuat Tanda Tangan Elektronik tersertifikasi dalam proses penyimpanan Data Pembuatan Tanda Tangan Elektronik; dan
- c. Memastikan mekanisme yang digunakan untuk penggunaan Data Pembuatan Tanda Tangan Elektronik untuk Tanda Tangan Elektronik menerapkan kombinasi paling sedikit 2 (dua) faktor autentikasi.

Pasal 64 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menjelaskan sebelum Tanda Tangan Elektronik digunakan, Penyelenggara Sertifikasi Elektronik wajib memastikan identifikasi awal Penanda Tangan dengan cara:

- a. Penanda Tangan menyampaikan identitas kepada Penyelenggara Sertifikasi Elektronik;
- b. Penanda Tangan melakukan registrasi kepada Penyelenggara Sertifikasi Elektronik; dan
- c. Dalam hal diperlukan, Penyelenggara Sertifikasi Elektronik dapat melimpahkan secara rahasia data identitas Penanda Tangan kepada Penyelenggara Sertifikasi Elektronik lainnya dengan persetujuan Penanda Tangan.

Pasal 58 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menjelaskan, Penyelenggara Sertifikasi Elektronik Indonesia menanggung kerugian yang diakibatkan oleh kesengajaan atau kelalaian kepada Orang, Badan Usaha atau Instansi karena kegagalannya dalam mematuhi kewajibannya sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Apabila penyelenggara sertifikasi elektronik Indonesia bekerjasama dengan penyelenggara sistem elektronik lain dalam penyelenggaraan sebagian infrastruktur atau layanannya, maka kerugian atau kelalaian yang terjadi tetap menjadi tanggungjawab penyelenggara sertifikasi elektronik Indonesia. Jika terbukti adanya kerugian atau kelalaian yang ditimbulkan oleh penyelenggara sertifikasi elektronik pada layanan Tanda Tangan Digital, maka hal yang harus dilaksanakan adalah bertanggung jawab atas hal yang terjadi. Penyelenggara sertifikasi elektronik juga memiliki hak untuk berpendapat dan membuktikan jika tidak menimbulkan kerugian.

2. Perlindungan Hukum Pengguna Tanda Tangan Digital Tersertifikasi

Pengguna Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik seperti dijelaskan pada Pasal 1 angka 11 PSTE. Pengguna Tanda Tangan Digital ini dapat diberikan pada setiap orang sesuai syarat. Yang dapat juga disebut konsumen dan dilindungi Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Transaksi elektronik Pasal 1 angka 2 UU ITE adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Adanya kesepakatan pada transaksi elektronik yang dijalankan oleh pelaku usaha dan konsumen menimbulkan kontrak atau hubungan hukum antara para pihak tersebut. Jika konsumen sepakat akan syarat-syarat dan klausula yang diajukan oleh penjual, maka terjadilah perjanjian walaupun perjanjian jual beli tersebut disepakati melalui tanda tangan yang bersifat elektronik.¹⁷

Kontrak elektronik sebagaimana kontrak konvensional pada umumnya, pembentukan kesepakatannya juga melalui tahap penawaran dan akseptasi. Ada dua jenis sarana komunikasi dalam proses tawar-menawar dibedakan dari durasi yang dibutuhkan, yakni komunikasi cepat (*Instantaneous Communications*) dan komunikasi lambat (*Non-Instantaneous Communications*). Dalam proses tawar-menawar yang dilakukan dengan alat komunikasi elektronik seperti telex, fax, dan surel, perbedaan waktu tidak setajam dalam kasus akseptasi melalui surat atau telegram. Sebuah kontrak elektronik terbentuk dengan sarana komunikasi yang bergerak sangat cepat, sehingga tidak mudah untuk menentukan waktu terjadinya saat akseptasi. Kaitan dengan waktu terjadinya akseptasi, *Principles of International Commercial Contracts (PICC)* menentukan bahwa penawaran harus diakseptasi sesuai dengan waktu yang ditetapkan (dalam penawarannya) atau jika tidak ditentukan waktu yang pasti, maka akseptasi harus diberikan dalam tenggang waktu yang patut (*Reasonable Time*) sesuai dengan keadaan dan kecepatan sarana komunikasi yang digunakan oleh pihak yang menawarkan.¹⁸

¹⁷ Agus R., *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Penerbit Citra Aditya Bakti, Bandung, 2007, p.91.

¹⁸ Y. Sogar Simamora, *Hukum Perjanjian: Prinsip Hukum Kontrak Pengadaan Barang dan Jasa oleh Pemerintah*, Penerbit LaksBang PRESSindo, Yogyakarta, 2009, p.206.

Hal serupa juga dikemukakan oleh UNCITRAL yang mendefinisikan *E-Commerce* sebagai berikut: “*Electronic commerce. Which involves the use of alternatives to paper-based of communication and storage of information*”. Vladimir Zwass, mendefinisikan transaksi *E-Commerce* sebagai pertukaran informasi bisnis, mempertahankan hubungan bisnis dan melakukan transaksi bisnis melalui jaringan komunikasi.¹⁹ Mengamati hal tersebut, transaksi *E-Commerce* adalah transaksi perdagangan jual beli barang dan jasa yang dilakukan dengan cara pertukaran informasi atau data menggunakan alternatif selain media tertulis. Yang dimaksud media transaksi di sini adalah media elektronik, khususnya internet. Jenis transaksi *E-Commerce* dibagi menjadi lima, yaitu²⁰:

- a. *Business to Business (B2B)*
Transaksi B2B merupakan transaksi, di mana kedua belah pihak yang melakukan transaksi adalah suatu perusahaan;
- b. *Business to Consumer (B2C)*
Transaksi B2C, merupakan transaksi antara perusahaan dengan konsumen atau individu. Transaksi B2C meliputi pembelian produk secara langsung oleh konsumen melalui internet;
- c. *Customer to Customer (C2C)*
Transaksi C2C merupakan transaksi, di mana individu saling menjual barang satu sama lain;
- d. *Customer to Business (C2B)*
Transaksi C2B, merupakan transaksi yang memungkinkan individu menjual barang pada perusahaan;
- e. *Customer to Government (C2G)*
Transaksi C2G merupakan transaksi, di mana individu dapat melakukan transaksi dengan pemerintah.

Konsep Tanda Tangan Digital (*Digital Signature*) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu tanda yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani. Dalam dunia nyata, untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan. Tanda tangan ini merupakan suatu tanda yang bersifat unik milik seseorang dan digunakan untuk memberi pengesahan bahwa orang itu setuju dan mengakui isi dari dokumen yang ditandatangani.²¹

¹⁹ Ridwan Khairandy, *Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Elektronik Commerce*, Jurnal Hukum Ius Quia Iustum, Vol.8, No.16 (2001), p.57-65.

²⁰ Roberto Aaron dkk., *Electronic Commerce: Enablers and Implications*, IEEE Communication Magazine, Vol.37, Issue 9 (1999), p.47.

²¹ Joan Venzka Tahapary, *Op.Cit.*, p.28.

Dalam proses penandatanganan elektronik, digunakan algoritma *Hash* untuk mencapai efisiensi sekaligus memastikan integritas suatu dokumen elektronik. Algoritma *Hash* adalah suatu rumus matematis yang mengoperasikan suatu pesan dengan panjang tertentu dan mengubahnya dalam bentuk yang lebih pendek.²² Dokumen-dokumen elektronik pun dibutuhkan hal semacam ini.

Oleh karena itu, diciptakan suatu sistem autentikasi yang disebut Tanda Tangan Digital. Tanda Tangan Digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda Tangan Digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.²³

Penyelenggaraan tanda tangan elektronik oleh PrivyID mengikuti ketentuan dalam UU ITE yang mensyaratkan pemenuhan aspek keamanan dokumen elektronik yakni keaslian (*Authentication*), keutuhan (*Integrity*), dan nirsangkal (*Non-Repudiation*). Proses penandatanganan diawali dengan pendaftaran pada *platform* penyelenggara tanda tangan elektronik. Pada proses ini, pengguna memasukkan data meliputi nama, alamat email, nomor ponsel, serta mengunggah foto Kartu Tanda Penduduk (KTP).²⁴

Kemudian, pengguna menunggu email konfirmasi registrasi dan melakukan verifikasi keabsahan dokumen identitas. Proses ini dilakukan untuk memastikan bahwa seluruh data pada saat proses penandatanganan elektronik berada dalam kuasa pengguna (penanda tangan) saja. Tahap selanjutnya setelah registrasi dan verifikasi ialah pengguna mengunggah dokumen yang hendak ditandatangani. Pada proses penandatanganan ini, terdapat sertifikat elektronik yang dapat menunjukkan bahwa segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui.²⁵

²² Jay Forder dan Dan Svantesson, *Internet and E-Commerce Law*, Penerbit Oxford University Press, Oxford, 2008, p.62.

²³ Joan Venzka Tahapary, *Op.Cit.*, p.28.

²⁴ Rizki Sulistio, 'The Role & Advantages of Digital Signature for the Fintech Industry', Sharing Session PrivyID, PrivyID, 2019. dalam Affan Muhammad Andalan, *Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial*, Jurist Diction, Vol.2, No.6 (November 2019), p.1943.

²⁵ Rizki Sulistio, 'The Role & Advantages of Digital Signature for the Fintech Industry', Sharing Session PrivyID, PrivyID, 2019. dalam Affan Muhammad Andalan, *Ibid.*.

Terdapat keterangan waktu mengenai kapan tanda tangan elektronik tersebut dibubuhkan dan rentang waktu keabsahannya. Di samping informasi mengenai perubahan terhadap tanda tangan elektronik, pengguna juga dapat mengetahui apabila ada perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan. Platform penyelenggara tanda tangan elektronik akan memunculkan informasi mengenai validitas identitas penandatanganan, waktu penandatanganan, dan kondisi orisinalitas dokumen yang ditandatangani.²⁶

Pasal 26 ayat (1) PP PSTE menyatakan penyelenggara sistem elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan. Penyelenggara sistem elektronik wajib melindungi pengguna dan masyarakat luas dari kerugian yang ditimbulkan oleh sistem elektronik yang diselenggarakannya. Disini jelas bahwa penyelenggara sertifikasi pada Tanda Tangan Digital harus dilindungi haknya, terkhusus dalam hal perlindungan data pribadi. Pasal 1 angka 29 PP PSTE menjelaskan bahwa data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik.

Dalam Pasal 29 PP PSTE, penyelenggara sistem elektronik wajib memberi informasi kepada pengguna sistem elektronik paling sedikit mengenai:

- a. Identitas Penyelenggara Sistem Elektronik;
- b. Objek yang ditransaksikan;
- c. Kelaikan atau keamanan Sistem Elektronik;
- d. Tata cara penggunaan perangkat;
- e. Syarat kontrak;
- f. Prosedur mencapai kesepakatan;
- g. Jaminan privasi dan/atau perlindungan Data Pribadi; dan
- h. Nomor telepon pusat pengaduan.

Pasal 45 ayat (1) PP PSTE menjelaskan mengenai transaksi elektronik yang dilakukan para pihak memberikan akibat hukum kepada para pihak dan dilanjut pada ayat (2) penyelenggaraan transaksi elektronik harus memperhatikan:

²⁶ Rizki Sulistio, 'The Role & Advantages of Digital Signature for the Fintech Industry', Sharing Session PrivyID, PrivyID, 2019. dalam Affan Muhammad Andalan, *Ibid.*

- a. Itikad baik;
- b. Prinsip kehati-hatian;
- c. Transparansi;
- d. Akuntabilitas; dan
- e. Kewajaran.

Pasal-pasal di atas menjelaskan pengguna Tanda Tangan Digital yang sudah tersertifikasi dapat dilindungi, memperoleh jaminan privasi dan/atau perlindungan pada data pribadi. Para pihak selanjutnya dalam berkegiatan transaksi elektronik haruslah memperhatikan itikad baik, memiliki prinsip kehati-hatian, transparan, akuntabilitas dan kewajaran. Pengguna dan penyelenggara sertifikasi elektronik harus saling menjalankan perannya masing-masing dengan baik.

Perlindungan terhadap data pribadi diatur lebih lanjut pada Pasal 58 ayat (1) PMSE menjelaskan setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau pelaku usaha yang bersangkutan. Diuraikan pada Pasal 59 PMSE:

- (1) Pelaku Usaha wajib menyimpan data pribadi sesuai standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang.
- (2) Standar perlindungan data pribadi atau kelaziman sebagaimana dimaksud pada ayat (1) paling sedikit memenuhi kaidah perlindungan:
 - a. Data pribadi harus diperoleh secara jujur dan sah dari pemilik data pribadi yang bersangkutan disertai dengan adanya pilihan dan jaminan adanya upaya pengamanan dan pencegahan kerugian pemilik data tersebut;
 - b. Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang dideskripsikan secara spesifik dan sah serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut;
 - c. Data pribadi yang diperoleh harus layak, relevan, dan tidak terlalu luas dalam hubungannya dengan tujuan pengolahannya sebagaimana disampaikan sebelumnya kepada pemilik data;
 - d. Data pribadi harus akurat dan harus selalu *up-to-date* dengan memberikan kesempatan kepada pemilik data untuk memutakhirkan data pribadinya;
 - e. Data pribadi harus diproses sesuai dengan tujuan perolehan dan peruntukannya serta tidak boleh dikuasai lebih lama dari waktu yang diperlukan;
 - f. Data pribadi harus diproses sesuai dengan hak subyek pemilik data sebagaimana diatur dalam peraturan perundang-undangan;
 - g. Pihak yang menyimpan data pribadi harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran atau mencegah setiap kegiatan pemrosesan atau pemanfaatan data pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi tersebut; dan
 - h. Data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia.

- (3) Dalam hal pemilik data pribadi menyatakan keluar, berhenti berlangganan atau berhenti menggunakan jasa dan sarana PMSE, maka pemilik data pribadi berhak meminta Pelaku Usaha untuk menghapus seluruh data pribadi yang bersangkutan.
- (4) Atas permintaan pemilik data pribadi sebagaimana dimaksud pada ayat (3), Pelaku Usaha harus menghapus seluruh data pribadi yang bersangkutan pada sistem yang dikelola oleh Pelaku Usaha tersebut.

Pelaku usaha pada kegiatan transaksi elektronik wajib menjaga data pribadi.

Data pribadi juga diatur pada Pasal 26 ayat (1) UU ITE yang menjelaskan:

Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. Setiap Orang yang melanggar haknya sebagaimana dimaksud tersebut dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan peraturan perundang-undangan.

Langkah hukum terakhir untuk mendapatkan perlindungan hukum dapat dilakukan dengan menempuh jalur penyelesaian sengketa. Penyelesaian sengketa dapat dilakukan pengguna Tanda Tangan Digital jika terjadi pelanggaran atau kerugian yang dilakukan penyelenggara sertifikasi elektronik. Pasal 38 ayat (1) UU ITE menjelaskan setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian. Selanjutnya, ayat (2) menjelaskan masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Selain penyelesaian gugatan perdata, para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan seperti diatur pada Pasal 39 ayat (1) dan ayat (2) UU ITE. Demikian halnya dengan pihak ketiga (*Intermediary*) yang terkait yang memberikan kontribusi sehingga secara teknis suatu transaksi perdagangan (*E-Commerce*) menjadi dapat dilakukan secara elektronik. Kerjasama antara para pihak terkait tersebut dalam suatu penyelenggaraan sistem elektronik untuk transaksi perdagangan harus dibangun dari semangat kerja sama yang saling menguntungkan dan bertanggung jawab secara tanggung renteng dan/atau bertanggung jawab secara proporsional kepada para pengguna sistem tersebut sesuai fungsi dan perannya masing-masing.

C. PENUTUP

1. Kesimpulan

Kekhawatiran masyarakat pada penggunaan Tanda Tangan Digital berkelindan mengenai pencurian data pribadi pengguna yang dapat disalahgunakan pihak yang tidak bertanggung jawab. Penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana diatur pada undang-undang. PSrE memiliki kewajiban salah satunya yaitu menjaga kerahasiaan identitas pemilik sertifikat elektronik dari pihak yang tidak memiliki kepentingan. Jika tidak dilaksanakan dengan baik oleh penyelenggara sertifikasi maka akan ada sanksi administratif sebagai konsekuensinya.

Pengguna Tanda Tangan Digital yang sudah tersertifikasi dapat dilindungi dan memperoleh jaminan privasi dan/atau perlindungan dalam hal data pribadi. Para pihak selanjutnya dalam berkegiatan transaksi elektronik haruslah memperhatikan itikad baik, memiliki prinsip kehati-hatian, transparan, akuntabilitas dan kewajaran. Upaya terakhir yang dapat ditempuh jika terjadi sengketa adalah melalui gugatan di pengadilan dan melalui mekanisme alternatif penyelesaian sengketa lainnya.

2. Saran

Harapannya, pemahaman masyarakat mengenai Tanda Tangan Digital yang tersertifikasi semakin baik sehingga dapat mendorong masyarakat khususnya di daerah untuk mempermudah kegiatan sehari-hari dalam bertransaksi elektronik. Meningkatkan sosialisasi dan edukasi kepada masyarakat dalam hal pentingnya penyelenggaraan sistem elektronik di era digital dan era pandemi ini. Tanggung jawab penyelenggara sertifikasi elektronik yang baik memberikan kepercayaan dan kenyamanan pada masyarakat sebagai pengguna. Diperlukan pengawasan dari pihak terkait untuk mengawasi penyelenggaraan sistem elektronik dan melindungi masyarakat pengguna Tanda Tangan Digital. Mendorong lahirnya aturan terkait perlindungan data pribadi yang saat ini masih belum secara khusus diatur pada peraturan undang-undang. Adanya pengawasan dan peraturan khusus terkait perlindungan data pribadi akan menciptakan suasana penyelenggaraan sistem elektronik yang kondusif di Indonesia.

DAFTAR PUSTAKA

Buku

- Busro, Achmad. 2011. *Hukum Perikatan Berdasarkan Buku III KUH Perdata*. (Yogyakarta: Penerbit Pohon Cahaya).
- Forder, Jay dan Dan Svantesson. 2008. *Internet and E-Commerce Law*. (Oxford: Penerbit Oxford University Press).
- Harahap, Yahya. 2015. *Hukum Acara Perdata: Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan*. (Jakarta: Penerbit Sinar Grafika).
- Kadir, Abdul. 2000. *Hukum Perdata Indonesia*. (Bandung: Citra Aditya Bakti).
- Marzuki, Peter Mahmud. 2016. *Penelitian Hukum*. (Jakarta: Penerbit Prenadamedia Group).
- Partodihardjo, Soemarno. 2009. *Tanya Jawab Sekitar Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. (Jakarta: Penerbit Gramedia Pustaka Utama).
- R., Agus. 2007. *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. (Bandung: Penerbit Citra Aditya Bakti).
- Raditio, Reza. 2014. *Aspek Hukum Transaksi Elektronik: Perikatan, Pembuktian dan Penyelesaian Sengketa*. (Yogyakarta: Penerbit Cipta Bakti).
- Simamora, Y. Sogar. 2009. *Hukum Perjanjian: Prinsip Hukum Kontrak Pengadaan Barang dan Jasa oleh Pemerintah*. (Yogyakarta: Penerbit LaksBang PRESSindo).

Publikasi

- Aaron Roberto, dkk.. *Electronic Commerce: Enablers and Implications*. IEEE *Communication Magazine*. Vol.37. Issue 9 (1999).
- Andalan, Affan Muhammad. *Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial*. *Jurist Diction*. Vol.2. No.6 (November 2019).
- Khairandy, Ridwan. *Pembaharuan Hukum Kontrak Sebagai Antisipasi Transaksi Elektronik Commerce*. *Jurnal Hukum Ius Quia Iustum*. Vol.8. No.16 (2001).
- Usman, Thamaroni. *Keabsahan Tanda Tangan Elektronik Pada Perjanjian Jual Beli Barang dari Perspektif Hukum Perdata*. *Indonesia Private Law Review*. Vol.1. Issue 2 (Juli-Desember 2020).

Karya Ilmiah

- Tahapary, Joan Venzka. 2011. *Keabsahan Tanda Tangan Elektronik Sebagai Alat Bukti yang Sah Ditinjau Dalam Hukum Acara Perdata*. Tesis. (Depok: Fakultas Hukum Universitas Indonesia).

Website

- Bagian Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat Badan Siber dan Sandi Negara. *Tanda Tangan Elektronik Si Mata Pena "The New Normal" Semangat Wujudkan Transformasi Digital Pemerintah*. diakses dari <https://bssn.go.id/tanda-tangan-elektronik-si-mata-pena-the-new-normal-semangat-wujudkan-transformasi-digital-pemerintah/>. diakses pada 20 April 2021.

Dinas Komunikasi Informatika dan Statistik Kabupaten Ponorogo. *Tanda Tangan Elektronik vs Tanda Tangan Digital*. diakses dari <https://kominfo.ponorogo.go.id/tanda-tangan-elektronik-vs-tanda-tangan-digital/>. diakses pada 19 April 2021.

Kementerian Komunikasi dan Informatika Republik Indonesia. *Apa Itu Penyelenggara Sertifikasi Elektronik*. diakses dari <https://tte.kominfo.go.id/apaitu#sebuah-perkenalan>. diakses pada 20 April 2021.

Kementerian Komunikasi dan Informatika Republik Indonesia. *Status Pengakuan Penyelenggara Sertifikasi Elektronik*. diakses dari <https://tte.kominfo.go.id/listPSrE/>. diakses pada 19 April 2021.

Privy Indonesia. *Tanda Tangan Elektronik vs Tanda Tangan Digital*. diakses dari <https://blog.privy.id/tanda-tangan-elektronik-vs-tanda-tangan-digital/>. diakses pada 19 April 2021.

Wijayanti, Ita. *Pemerintahan Berbasis Elektronik dalam Pelayanan Publik*. diakses dari <https://ombudsman.go.id/artikel/r/artikel--pemerintahan-berbasis-elektronik-dalam-pelayanan-publik>. diakses pada 20 April 2021.

Sumber Hukum

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42. Tambahan Lembaran Negara Republik Indonesia Nomor 3821.

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

Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 45. Tambahan Lembaran Negara Republik Indonesia Nomor 5512.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185. Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 222. Tambahan Lembaran Negara Republik Indonesia Nomor 6420.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik. Berita Negara Republik Indonesia Tahun 2018 Nomor 1238.